EXHIBIT A

CHRISTOPHER GRIVAKES
cg@agzlaw.com
DAMION ROBINSON
dr@agzlaw.com
AFFELD GRIVAKES LLP
2049 Century Park East, Suite 2460
Los Angeles, CA 90067
Telephone: 310.979.8700
Facsimile: 310.979.8701

Attorneys for Plaintiff ROBERT ROSS

THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ROBERT ROSS,

Plaintiff,

v.

AT&T MOBILITY, LLC, ONE TOUCH DIRECT, LLC, and ONE TOUCH DIRECT- SAN ANTONIO, LLC,

Defendants.

Case No. 4:19-cv-6669

FIRST AMENDED COMPLAINT

DEMAND FOR JURY TRIAL

I. NATURE OF THE ACTION

1. This action arises out of AT&T's failure to protect the sensitive and confidential account data of its mobile service subscriber, Robert Ross, resulting in massive violations of Mr. Ross's privacy, the compromise of his highly sensitive personal and financial information, and the theft of more than $1 million.

2. AT&T is the country's largest mobile service provider. Tens of millions of subscribers entrust AT&T with access to their confidential information, including information that can serve as a key to unlock subscribers' highly sensitive personal and financial information.

3. Recognizing the harms that arise when mobile subscribers' personal information is accessed, disclosed, or used without their consent, federal and state laws require AT&T to protect this sensitive information.

4. AT&T also recognizes the sensitivity of this data and promises its 150 million mobile subscribers that it will safeguard their private information – and particularly their data-rich SIM cards – from any unauthorized disclosure. AT&T promises it "will protect [customers'] privacy and keep [their] personal information safe" and that it "will not sell [customers'] personal information to anyone, for any purpose. Period." AT&T repeatedly broke these promises.

5. In an egregious violation of the law and its own promises, and despite advertising itself as a leader in technological development and as a cyber security-savvy company, AT&T breached its duty and promise to Mr. Ross to protect his account and the sensitive data it contained. AT&T failed to implement sufficient data security systems and procedures, instead allowing third parties to gain unauthorized access to Mr. Ross's AT&T account in order to steal from him.

6. AT&T's actions and conduct were a critical factor in causing significant financial and emotional harm to Mr. Ross and his family. But for AT&T employees', representatives' and agents' unauthorized access to Mr. Ross' account, and failure to protect Mr. Ross through adequate security and oversight systems

and procedures, Mr. Ross would not have had his personal privacy repeatedly violated and would not have been a victim of SIM swap theft.

7. Mr. Ross brings this action to hold AT&T accountable for its violations of federal and state law, and to recover for the grave financial and personal harm suffered by Mr. Ross and his family as a direct result of AT&T's acts and omissions, as detailed herein.

II. THE PARTIES

8. Plaintiff Robert Ross is, and at all relevant times was, a resident of California. Mr. Ross currently resides in San Francisco, California.

9. Mr. Ross was an AT&T mobile customer at all times relevant to this Complaint. He purchased a mobile phone plan from AT&T in San Francisco, California in 2007 for personal use, was an active, paying AT&T mobile subscriber at all times relevant to the allegations in this Complaint, and his business relationship was directly with AT&T at all relevant times.

10. Defendant AT&T Mobility, LLC (hereinafter, "AT&T") is a Delaware limited liability corporation with its principal office or place of business in Brookhaven, Georgia. AT&T "provides nationwide wireless services to consumers and wholesale and resale wireless subscribers located in the United States or U.S. territories" and transacts or has transacted business in this District and throughout the United States. It is the second largest wireless carrier in the United States, with more than 153 million subscribers, earning $71 billion in total operating revenues in 2017 and $71 billion in 2018. As of December 2017, AT&T had 1,470 retail locations in California.[1]

11. AT&T provides wireless service to subscribers in the United States. AT&T is a "common carrier" governed by the Federal Communications Act ("FCA"), 47 U.S.C. § 151 *et seq*. AT&T is regulated by the Federal

[1] "About Us," AT&T, *available at* https://engage.att.com/california/about-us/. This URL was last accessed on October 15, 2019.

Communications Commission ("FCC") for its acts and practices, including those occurring in this District.

12. AT&T Inc., AT&T's parent company, acknowledged in its 2018 Annual Report that its "profits and cash flow are largely driven by [its] Mobility business" and "nearly half of [the] company's EBITDA (earnings before interest, taxes, depreciation and amortization) come from Mobility."[2]

13. Defendant One Touch Direct, LLC ("One-Touch Direct") is a Florida Corporation with its principal place of business in Tampa, Florida. Plaintiff is informed and believes and thereon alleges that AT&T contracted with One-Touch Direct to provide call center services for AT&T's mobile phone customers.

14. Defendant One Touch Direct - San Antonio, LLC ("One-Touch Direct-SA") is a Florida Corporation with its principal place of business in Tampa, Florida. Plaintiff is informed and believes and thereon alleges that One-Touch Direct-SA is a subsidiary of One Touch Direct - SA and the employer of the customer service representative(s) who executed the remote SIM swap on Plaintiff's mobile phone.

15. At all relevant times, One Touch Direct and One Touch Direct-SA were AT&T's authorized representatives and agents and performed services for AT&T which were within the usual course of AT&T's business.

16. At all relevant times, AT&T dictated and controlled the manner and means by which One Touch Direct and One Touch Direct-SA performed their services for AT&T. On information and belief, AT&T entered into a master services agreement with One Touch Direct which governed the terms and condition of AT&T's relationship with One Touch Direct and its subsidiaries such as One Touch Direct-SA, and which required the One Touch entities to strictly adhere to AT&T's guidelines, protocols, policies, and procedures relating to customer

[2] *Id.*

service, including those relating to SIM swaps. Furthermore, AT&T controlled the security measures it implemented across its entire network operation (including its own call centers and third-party call centers), as well as the data accumulated across the entire network, to monitor, detect and prevent unauthorized SIM swaps.

17. At all relevant times, One Touch Direct and One Touch Direct-SA employees identified themselves to Mr. Ross as "AT&T" rather than One Touch Direct (at AT&T's direction), had full access to and use of the AT&T customer database which enabled them to perform customer service functions (including SIM swaps), did not disclose that they were employed by One Touch Direct, and were in essence *de facto* employees of AT&T.

III. JURISDICTION AND VENUE

18. This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act ("FCA"). The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims because the claims are derived from a common nucleus of operative facts. The Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1332 because Mr. Ross is a citizen of a different state than AT&T, One Touch Direct, and One Touch Direct-SA.

19. This Court has personal jurisdiction over AT&T and its contractors One Touch Direct and One Touch Direct-SA because AT&T purposefully directs its conduct at California, transacts substantial business in California (including in this District), has substantial aggregate contacts with California (including in this District), engaged and is engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in California (including in this District), and purposely avails itself of the laws of California. AT&T had more than 33,000 employees in California as of 2017, and

1,470 retail locations in the state.[3] Mr. Ross purchased his AT&T mobile plan in California, visited AT&T retail locations in California, and was injured in California by the acts and omissions alleged herein.

20. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the conduct giving rise to Mr. Ross' claims occurred in this District and Defendant transacts business in this District. Mr. Ross purchased his AT&T mobile plan in this District and was harmed in this District, where he resides, by the acts and omissions of Defendants, as detailed herein.

IV. ALLEGATIONS APPLICABLE TO ALL COUNTS

21. As a telecommunications carrier, AT&T is entrusted with the sensitive mobile account information and personal data of millions of Americans, including Mr. Ross' confidential and sensitive personal and account information. AT&T's duties to safeguard customer information are non-delegable to any other entity, including its third-party call center service providers such as the One Touch Direct entities.

22. Despite its representations to its customers and its obligations under the law, AT&T has failed to protect Mr. Ross' confidential information. In October 2018, AT&T employees, representatives and agents obtained unauthorized access to Mr. Ross' AT&T mobile account, viewed his confidential and proprietary personal information, and transferred control over Mr. Ross' AT&T mobile number and service from Mr. Ross' phone to a phone controlled by third-party hackers. The hackers then immediately utilized their control over Mr. Ross' AT&T mobile number—control secured with necessary and direct assistance from AT&T employees, representatives and agents —to access and take control of his personal and digital finance accounts and steal $1 million from Mr. Ross.

[3] "About Us," AT&T California, *supra* at 1.

23. This type of telecommunications account hacking behavior is known as "SIM swapping."

A. SIM Swapping is a Type of Identity Theft Involving the Transfer of a Mobile Phone Number

24. Mr. Ross was the victim of an unauthorized "SIM swap" on October 26, 2018.

25. A "SIM swap" is a relatively simple scheme, wherein a hacker gains control of a victim's mobile phone number and service in order to intercept communications, including text messages, intended for the victim. The hackers then use that phone number as a key to access and take over the victim's digital accounts, such as email, file storage, and financial accounts.

26. Most mobile phones, including the iPhone owned by Mr. Ross at the time of his SIM swap, have an internal SIM ("subscriber identity module") card. A SIM card is a small, removable chip that allows a mobile phone to communicate with the mobile carrier's network and the carrier to know what subscriber account is associated with that mobile phone. The connection between the mobile phone and the SIM card is made through the carrier, which associates each SIM card with the physical phone's IMEI ("international mobile equipment identity"), which is akin to the mobile phone's serial number. Without an activated SIM card and effective SIM connection, a mobile phone typically cannot send or receive calls or text messages over the carrier network. SIM cards can also store a limited amount of account data, including contacts, text messages, and carrier information, and that data can help identify the subscriber.

27. The SIM card associated with a mobile phone can be changed. If a carrier customer buys a new phone that requires a different sized SIM card, for example, the customer can associate his or her account with a new SIM card and the new phone's IMEI by working with their mobile carrier to effectuate the change. This allows carrier customers to move their mobile number from one

mobile phone to another and to continue accessing the carrier network when they switch mobile phones. For a SIM card change to be effective, the carrier is required by law to authenticate that the change request is legitimate and actualize the change. AT&T allows its employees, representatives and agents to conduct SIM card changes for its customers remotely or in its retail stores, and does so numerous times daily with inadequate protections against unauthorized SIM swaps.

28. An unauthorized SIM swap refers to an illegitimate SIM card change. During a SIM swap attack, a carrier representative switches the SIM card number associated with the victim's mobile account from the victim's phone to a phone controlled by a hacker. This literally re-routes the victim's mobile phone service — including any incoming data, texts, and phone calls associated with the victim's phone — from the victim's physical phone to a physical phone controlled by the hacker. The hacker's phone then becomes the phone associated with the victim's carrier account, and the hacker receives all of the text messages and phone calls intended for the victim.[4] Simultaneously, the victim's mobile phone loses its ability to connect to the carrier network and displays "No Service".

29. Once hackers are given control over the victim's phone number, they can immediately use that control to access and take complete control of the victim's personal online accounts, such as email and banking accounts, through exploiting password reset links and codes sent via text message to the now-hacker-controlled-phone or the two-factor authentication processes associated with the victim's digital accounts. Two-factor authentication allows digital accounts to be

[4] As described by federal authorities in prosecuting SIM swap cases, SIM swapping enables hackers to "gain control of a victim's mobile phone number by linking that number to a subscriber identity module ('SIM') card controlled by [the hackers]—resulting in the victim's phone calls and short message service ('SMS') messages being routed to a device controlled by [a hacker]." *United States of America v. Conor Freeman, et al.*, No. 2:19-cr-20246-DPH-APP (E.D. Mich. Filed Apr. 18, 2019) (hereafter, "Freeman Indictment") (attached hereto as Exhibit A), ECF. No. 1 at ¶ 3.

accessed without a password or allows the account password to be changed. One common form of two-factor authentication enabled, allowed, and used by AT&T itself is through text messaging. Rather than enter a password, the hacker requests that a password reset link or code be sent to the mobile phone number associated with the victim's online account which AT&T makes possible. Because the hacker now controls the victim's phone number, the reset code is sent to the hacker. The hacker can then log into, and change the password for, the victim's account, allowing the hacker to access and take complete control of the contents of the account.[5]

30. Therefore, obtaining access to and control over a victim's mobile phone service is the central part of breaking into the victim's other online accounts, such as email services or financial accounts. The sole reason for the fraudulent SIM swap is for the hackers to take control of the victims' financial and online accounts that would not otherwise be accessible. A SIM swap is an extremely high-risk transaction, as it directly enables the hacker to take control of a victim's life.

31. The involvement of a SIM swap victim's mobile carrier is critical to an unauthorized SIM swap. In order for an unauthorized SIM swap to occur and for a SIM swap victim to be at any risk, the carrier must pro-actively and intentionally activate the SIM card in the hacker's phone, which simultaneously results in the SIM card in the victim's phone to be deactivated. At that point, the victim's phone will display "No Service" as their phone can no longer connect to the carrier's network.

32. Upon information and belief, in Mr. Ross's case, not only did AT&T employees, representatives and agents access his account without authorization,

[5] *See, e.g.*, *Id.* at ¶ 4 ("Once [hackers] had control of a victim's phone number, it was leveraged as a gateway to gain control of online accounts such as the victim's email, cloud storage, and cryptocurrency exchange accounts. Sometimes this was achieved by requesting a password-reset link be sent via [text messaging] to the device control by [hackers]. Sometimes passwords were compromised by other means, and [the hacker's] device was used to received two-factor authentication ('2FA') message sent via [text message] intended for the victim.").

they also changed his SIM card number to a phone controlled by hackers, who then immediately used that control to steal from Mr. Ross and access sensitive personal information.

B. AT&T Facilitated Unauthorized Access to Mr. Ross' AT&T Account and Gave Control of His Account to Hackers

33. AT&T employees, representatives and agents accessed Mr. Ross' AT&T mobile account without his authorization, obtained his confidential and proprietary personal information, and gave complete control of his mobile service to hackers – all without Mr. Ross' knowledge or consent. Those hackers then immediately used their control over Mr. Ross' mobile phone number to access and take control of his sensitive and confidential information and accounts and steal more than $1 million from him and access sensitive personal information such as passports, drivers' licenses and birth certificates.

34. On October 26, 2018 at approximately 6:00 PM PT, Mr. Ross began receiving notifications that someone was attempting to withdraw currency from his account at Gemini, a provider of financial services. This caused Mr. Ross significant distress because, at the time, Mr. Ross had $500,000 in USD in his Gemini account.

35. At approximately the same time, Mr. Ross noticed that his AT&T mobile phone had lost service and displayed "No Service", and he also noticed that he was automatically logged out of his Gmail account.

36. Mr. Ross immediately suspected that a hacker attack was underway and took his mobile phone to an Apple store for assistance.

37. Apple representatives assisted Mr. Ross in contacting AT&T Customer Support. At that time, an AT&T employee, representative and agent informed the Apple representatives that Mr. Ross' SIM card had been changed. AT&T employees, representatives and agents advised the Apple representatives to provide Mr. Ross with a new SIM card, and then Apple employees replaced the SIM card

in Mr. Ross' phone. AT&T then activated the new SIM card, restoring Mr. Ross' access to his AT&T mobile number and account services.

38. When Mr. Ross returned home that evening, he called AT&T's customer service to discuss the unauthorized access to his account by AT&T employees, representatives and agents and the unauthorized SIM swap. An AT&T customer service representative who identified himself as Ryan S. (with a representative identification number RS410M) informed Mr. Ross that an unauthorized SIM swap had occurred on his service at approximately 5:47 PM PT by AT&T representative Cristelo V. (with a representative identification number CV921H).

39. AT&T representative Ryan S. also informed Mr. Ross that this unauthorized SIM swap request was made using customer owned and maintained equipment ("COAM"), and explained that COAM is a mobile phone that is not provided by AT&T and would generally be of unknown origin to AT&T (for example, a hacker might purchase a used mobile phone on the internet). Furthermore, Ryan S. expressed surprise that this SIM swap was executed as he told Mr. Ross it was against AT&T internal policies for an AT&T representative to execute a COAM-originated SIM swap request from anyone calling in to an AT&T call center. Ryan S further represented that he made a specific note of this violation of AT&T's own policy in Mr. Ross' account, reading the note verbally to Mr. Ross "I have informed customer that a SIM card and IMEI change occurred on 10/26/18 at 5:47pm. This change was approved by agent which is a direct violation of the ATT activation policy." After a couple of hours on this call, Ryan S told Mr. Ross that his supervisor would take over the call, which she did, and immediately told Mr. Ross that Ryan S should not have given the information he did to Mr. Ross, and she immediately and abruptly terminated the call, causing further distress to Mr. Ross.

40. AT&T employees, representatives and agents (including Ryan S.) represented to Mr. Ross that AT&T would place a warning on his account stating that he was experiencing fraud and instructing AT&T employees not to change anything on his account – including his SIM card.

41. AT&T informs its customers that verbal account passcodes—which are different than online account sign-in passwords or the passcodes used to access a mobile device—are used to protect customer's mobile accounts and may be required when a customer manages their AT&T account online or in an AT&T store.[6]

42. Within minutes of AT&T giving control over Mr. Ross's AT&T mobile number to the hackers, they used that control to access and take over Mr. Ross' accounts at his financial services providers, including but not limited to, Coinbase, Gemini, and Binance. Coinbase and Gemini allow their users to store US dollars that can be used to buy and sell cryptocurrencies (such as bitcoin) within the user's account, in a similar way to how users can store US dollars used to buy and sell stocks at financial services providers such as Fidelity, Schwab, and E*Trade.

43. At the time of the SIM swap attack, Mr. Ross had approximately $500,000 in US dollars in his Gemini account and approximately $500,000 in US dollars in his Coinbase account. By utilizing their control over Mr. Ross' mobile phone number, which AT&T gave them, third-party hackers were able to access and take control of these accounts of Mr. Ross and control the entire USD amounts he held in both accounts. The hackers used Mr. Ross's $1,000,000 in US dollars to purchase bitcoin—a type of cryptocurrency that can be difficult to trace—and then the hackers transferred that bitcoin into accounts they controlled at a different

[6] "Get info on passcodes for mobile accounts," AT&T, *available at* https://www.att.com/esupport/article.html#!/mobile/KM1049472?gsi=tp3wtr.

financial services provider. This made the cryptocurrency exceedingly difficult to trace, let alone recover.[7]

44. The hackers also transferred cryptocurrency worth approximately $3,000 from Mr. Ross' Binance account into accounts they controlled, thereby stealing those funds from him as well.

45. The hackers also used their control over Mr. Ross' AT&T mobile phone number to access, change the passwords, and take control of several of Mr. Ross' most sensitive online accounts, including, but not limited to, his Authy, Google, Yahoo!, and DropBox accounts. In taking over his Google account, the hackers also changed his passwords and the phone number linked to Mr. Ross' two-factor authentication for these accounts, which made it impossible for Mr. Ross to regain immediate access to, let alone control of, these accounts (because any requests to remind him of or reset the password no longer were sent to Mr. Ross' mobile phone, but rather to the hacker's phone). It took Mr. Ross approximately 7-10 days to regain access to and restore control over his email and, and longer for his other online personal accounts, and several weeks to regain access to the accounts taken over at his other financial services providers. In addition, the hackers deleted several weeks-worth of emails and substantial data from Mr. Ross' Google account. Mr. Ross has not been able to recover any of this data.

46. Criminal investigations by the California-based Regional Enforcement Allied Computer Team ("REACT"), a multi-jurisdictional law enforcement partnership specializing in cybercrime, into the October 2018 breach of Mr. Ross' AT&T account and the resulting theft revealed the involvement of a third-party

[7] *See* Investigation Report, Regional Enforcement Allied Computer Team, *California v. Nicholas Truglia* (Oct. 2018) (attached hereto as Exhibit B) at p. 8 ("explaining that "all of Robert R.'s funds stored in Coinbase (approximately $500,000) and Gemini (approximately $500,000) had been held in USD. The [hacker] used all the funds in USD at both exchanges to purchase bitcoins, then immediately withdrew all of the bitcoins. … This information was subsequently verified by obtaining records directly from Coinbase and Gemini via search warrant.").

hacker named Nicholas Truglia, who was arrested by REACT detectives on November 13, 2018, and faces 21 felony counts in Santa Clara County for SIM swaps and related thefts, including against Mr. Ross. In their investigation report, REACT detectives specifically wrote that they obtained a search warrant for AT&T records pertaining to these thefts, and in response, AT&T provided REACT investigators with records that showed the same mobile device used by the hacker (identified through the devices IMEI number) had been used to effect the account takeovers of Mr. Ross, as well as the accounts of several other victims. In total, the records indicated that, prior to the unauthorized and illegal SIM swap and theft facilitated by AT&T against Mr. Ross, 11 unique phone numbers had been SIM swapped using this device between October 5 and October 26, 2018. It is incredulous that AT&T not only allowed these other unauthorized SIM swaps to happen, resulting in several other victims, but certainly knew or should have known that the same mobile device used to SIM swap other victims was already being used by a hacker who later used that same device to SIM swap Mr. Ross. Even the most basic check by AT&T would have easily flagged this IMEI as being used to perpetrate completely unauthorized and illicit SIM swaps well prior to the unauthorized and illegal SIM swap against Mr. Ross, which resulted within 45 minutes of the theft of almost his entire life's savings of $1,000,000.

47. Mr. Ross' financial and personal life have been uprooted as a result of AT&T's failure to safeguard his account.

48. As a result of the SIM swap detailed above, Mr. Ross lost more than $1 million in USD. This money constituted the majority of Mr. Ross' life savings and the money he had saved for his daughter's college fund as well as his own retirement.

49. The financial strain resulting from the robbery of Mr. Ross has caused extreme emotional distress for Mr. Ross. The loss of his savings caused massive disruption in Mr. Ross' financial planning and caused him to worry about the

financial well-being of himself and his daughter. He has suffered, and continues to suffer, from severe anxiety, fear, weight gain, depression, and loss of sleep as a direct result.

50. Additionally, Mr. Ross' and his minor daughter's sensitive and confidential personal information have been compromised as a result of the SIM swaps. Mr. Ross stored color copies of their passports, drivers' licenses, and birth certificates in the online accounts which were taken over by the hackers as a result of the AT&T-facilitated SIM swap. Ten years of Mr. Ross' sensitive and confidential tax returns were also compromised. All of this information is now at extraordinarily high risk of being posted or bought and sold on the dark web by criminals and identity thieves, putting Mr. Ross and his minor child at ongoing risk of significant privacy violations, identity theft, and countless additional unknown harms for the rest of their lives.

C. AT&T's Failure to Protect Mr. Ross' Account from Unauthorized Access Violates Federal Law

51. AT&T is the world's largest telecommunications company and provider of mobile telephone services. As a common carrier,[8] AT&T is governed by the Federal Communications Act of 1934, as amended ("FCA"),[9] and corresponding regulations passed by the FCC.[10]

52. Recognizing the sensitivity of data collected by mobile carriers, Congress, through the FCA, requires AT&T to protect Mr. Ross' sensitive personal information to which it has access as a result of its unique position as a telecommunications carrier.[11]

53. Section 222 of the FCA, which became part of the Act in 1996, requires AT&T to protect the privacy and security of information about its

[8] 47 U.S. Code § 153(51).
[9] 47 U.S.C. § 151 *et seq.*
[10] 47 C.F.R. § 64.2001 *et seq.*
[11] 47 U.S.C. § 222.

customers. Likewise, Section 201(b) of the Act requires AT&T's practices related to the collection of information from its customers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.[12]

54. AT&T's most specific obligations to protect its customers concerns a specific type of information, called Customer Proprietary Information and Other Customer Information, and known by the acronym "CPNI."[13] Specifically, the FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."[14]

55. Carriers like AT&T are liable for failures to protect their customers unauthorized disclosures.[15] The FCC has also stated that "[t]o the extent that a carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of section 222 may have occurred."[16]

56. CPNI is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and . . . information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[17]

---

[12] 47 U.S.C. § 201(b).

[13] 47 U.S.C. § 222(a).

[14] Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd. 6927 ¶ 1 (April 2, 2007) (hereafter, "2007 CPNI Order").

[15] 47 U.S.C. §§ 206, 207.

[16] Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information*, 28 F.C.C. Rcd. 9609 ¶ 30 (2013) (hereafter, "2013 CPNI Order").

[17] 47 U.S.C. § 222(h)(1).

57. As AT&T has admitted to customers, SIM swap attacks constitute a CPNI breach.

58. Mr. Ross' CPNI was breached by one or more AT&T employees, representatives and agents when they accessed his account and swapped his SIM card number without his authorization. When employees, representatives and agents accessed Mr. Ross' account, his CPNI was visible. On information and belief, this included, but was not limited to, information about the configuration, type, and use of his subscribed AT&T services, his personal information, his SIM card details, and his billing information. AT&T employees, representatives and agents then used this information to effectuate an unauthorized SIM swap.

59. This type of unauthorized use of Mr. Ross' CPNI is illegal under the FCA. The FCA forbids AT&T from "us[ing], disclos[ing], or permit[ting] access to" CPNI, except in limited circumstances.[18] This extends to the carrier's employees, representatives and agents.

60. AT&T may only use, disclose, or permit access Mr. Ross' CPNI: (1) as required by law; (2) with his approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[19] Beyond such use, "the Commission's rules require carriers to obtain a customer's knowing consent before using or disclosing CPNI."[20]

61. AT&T failed to protect Mr. Ross from authorized use of his CPNI. AT&T permitted its employees, representatives and agents to use and/or disclose Mr. Ross' CPNI without obtaining Mr. Ross' knowing consent beforehand. AT&T employees, representatives and agents, acting within the scope of their employment and agency, likewise did not seek Mr. Ross' knowing consent before

[18] 47 U.S.C. § 222(c)(1).
[19] 47 U.S.C. § 222.
[20] 2007 CPNI Order ¶ 8 (emphasis added).

using, disclosing, and/or permitting access to his CPNI when they accessed his account and swapped his SIM card. Instead, AT&T employees, representatives and agents authorized a COAM SIM swap over the phone, in violation of AT&T's own internal policies. Because such conduct does not fit within the FCA's recognized legitimate uses, it constitutes a violation of the FCA.

62. Pursuant to the FCA, the FCC has developed comprehensive rules concerning AT&T's obligations under its duty to protect customers' CPNI.[21] This includes rules "designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI."[22] The FCC specifically recognizes that "[a]bsent carriers' adoption of adequate security safeguards, consumers' sensitive information… can be disclosed to third parties without consumers' knowledge or consent."[23] In a 2013 order, the FCC "clarif[ied] existing law so that consumers will know that *their carriers must safeguard these kinds of information so long as the information is collected by or at the direction of the carrier and the carrier or its designee*[24] *has access to or control over the information*."[25]

63. Pursuant to these rules, AT&T must "implement a system by which the status of a customer's CPNI approval can be clearly established *prior to* the use of CPNI."[26] AT&T is also required to "design their customer service records in such a way that the status of a customer's CPNI approval can be clearly

---

[21] *See* 47 CFR § 64.2001("The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222."). The FCC also regularly releases CPNI orders that promulgate rules implementing its express statutory obligations. *See* 2007 CPNI Order and 2013 CPNI Order.

[22] 2007 CPNI Order ¶ 9; *see also Id.* at ¶ 35; 47 U.S.C. § 222(c); 47 C.F.R. § 64.2009.

[23] *Id.*

[24] In the ruling, "designee" is defined as "an entity to which the carrier has transmitted, or directed the transmission of, CPNI or is the carrier's agent." *Id.* n. 1.

[25] *Id.* at ¶ 1 (emphasis added).

[26] 2007 CPNI Order ¶¶ 8-9 (emphasis added); *see also* 47 C.F.R. § 64.2009(a).

established."[27] The FCC's rules also "require carriers to maintain records that track access to customer CPNI records."[28]

64. Upon information and belief, AT&T has failed to implement such a system. The fact that Mr. Ross' account was accessed, and his SIM card number was changed without his authorization, demonstrates AT&T's failures in this regard.

65. AT&T is also required to "train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place."[29]

66. Upon information and belief, AT&T has failed to properly train and supervise its personnel, contractors, representatives and agents, as reflected by an AT&T employee, representative and agent's involvement in Mr. Ross' breaches – and that employee, representative's and agent's ability to so easily effectuate a SIM swap in violation of AT&T's own internal policies.

67. AT&T has also breached its duty to safeguard Mr. Ross' CPNI from data breaches, in violation of Section 222(a) and Section 201(b) of the FCA.

68. The FCC has "[made] clear that carriers' existing statutory obligations to protect their customers' CPNI include[s] a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI."[30]

69. AT&T failed to take reasonable steps to protect Mr. Ross' CPNI, thereby allowing third-party hackers to access his CPNI.

70. The FCC also requires that carriers inform customers – and law enforcement – "whenever a security breach results in that customer's CPNI being

---

[27] *Id.* ¶ 9.
[28] *Id.*
[29] 47 C.F.R. § 64.2009(b) "Safeguards required for use of customer proprietary network information".
[30] 2007 CPNI Order ¶ 36 (citation omitted).

disclosed to a third party without that customer's authorization."[31] This requirement extends to *any* unauthorized disclosure.

71. In adopting this requirement, the FCC rejected the argument that it "need not impose new rules about notice to customers of unauthorized disclosure because competitive market conditions will protect CPNI from unauthorized disclosure."[32]

72. Instead, the FCC found that "[i]f customers and law enforcement agencies are unaware of [unauthorized access], unauthorized releases of CPNI will have little impact on carriers' behavior, and thus provide little incentive for carriers to prevent further unauthorized releases. By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers and assist law enforcement with its investigations. This notice will also empower carriers and consumers to take whatever 'next steps' are appropriate in light of the customer's particular situation."[33] The FCC specifically recognized that this notice could allow consumers to take precautions or protect themselves "to avoid stalking or domestic violence."[34]

73. AT&T failed in its duty to safeguard Mr. Ross' CPNI from breaches and, upon information and belief, has failed to properly inform him of such breaches when they occurred. Mr. Ross never received any documentation or communication alerting him that his CPNI had been breached, even though AT&T knew his CPNI had been breached as a result of the REACT criminal investigation, and knew or should have known that his CPNI had been breached as a result of multiple prior SIM swaps enacted by hackers using the same mobile phone and IMEI.

---

[31] 2007 CPNI Order at ¶ 26; *see also* 47 C.F.R § 64.2011(c).
[32] 2007 CPNI Order ¶ 30.
[33] *Id.*
[34] *Id.* at n. 100.

74. Under the FCA, AT&T is not just liable for its own violations of the Act, but also for violations that it "cause[s] or permit[s]."[35] By failing to secure Mr. Ross' account and protect his CPNI, AT&T caused and/or permitted Mr. Ross' CPNI to be accessed and used by its own employees, representatives and agents and by third-party hackers.

75. AT&T is also responsible for the acts, omissions, and/or failures of officers, agents, employees, or any other person acting for or employed by AT&T.

D. Mr. Ross' Harm was Caused by Defendants' Negligence

76. By failing to secure Mr. Ross' account—and protect the confidential and sensitive data contained therein—and to properly hire, train, and supervise their employees, representatives and agents, Defendants are responsible for the foreseeable harm Mr. Ross suffered as a result of Defendants' gross negligence.

Further, Defendants are responsible for their representatives' and agents' failure to obtain Mr. Ross' valid consent before accessing his account and effectuating a SIM swap, as such actions were within the scope of their agency of employment with Defendants. On information and belief, Defendants' representatives and agents were tasked with and able to change customers' SIM card numbers at will – even when such changes violated AT&T company policy. Additionally, Defendants representatives' and agents' breach of Mr. Ross' account and the subsequent SIM swap was foreseeable. AT&T has known for more than a decade that third parties frequently attempt to access and take over mobile customers' accounts for fraudulent purposes.

[35] *See* 47 U.S.C.A. § 206 (establishing that "[i]n case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter[.]")

77. In 2007, the FCC issued an order strengthening its CPNI rules in response to the growing practice of "pretexting."[36] Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communication records."[37] This 2007 Order put AT&T on notice that its customers' accounts were vulnerable targets of the third-parties seeking unauthorized access.

78. AT&T and its representatives and agents also knew, or should have known, about the risk SIM swap crimes presented to its customers. SIM swap crimes have been a widespread and growing problem for years. The U.S. Fair Trade Commission ("FTC") reported in 2016 that there were 1,038 reported SIM swap attacks *per month* in January 2013, which increased sharply to 2,658 per month by January 2016—2.5 times as many.[38] The FTC reported that SIM swaps represented 6.3% of all identity thefts reported to the agency in January 2016, and that such thefts "involved all four of the major mobile carriers" – including AT&T.[39]

79. AT&T knew or should have known that it needed to take steps to protect its customers. The FTC's 2017 Report stated that "*mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking*[.]"[40] The FTC urged carriers like AT&T to "adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions."[41] The FTC also specifically warned carriers like AT&T of the risk that, due to text message

---

[36] 2007 CPNI Order.
[37] *Id.* at ¶ 1.
[38] Lori Cranor, FTC Chief Technologist, "Your mobile phone account could be hijacked by an identity thief," Federal Trade Commission (June 7, 2016), *available at* https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief (hereafter, "2017 FTC Report").
[39] *Id.*
[40] *Id.* (emphasis added).
[41] *Id.*

password reset requests and two-factor authentication, SIM swapping put subscribers at risk of financial loss and privacy violations:

> Having a mobile phone account hijacked can waste hours of a victim's time and cause them to miss important calls and messages. However, this crime is particularly problematic due to the growing use of text messages to mobile phones as part of authentication schemes for financial services and other accounts. The security of two-factor authentication schemes that use phones as one of the factors relies on the assumption that someone who steals your password has not also stolen your phone number. *Thus, mobile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.*[42]

80. AT&T admitted it was aware of SIM swap crimes and the effect they could have on its customers in September 2017 when AT&T's Vice President of Security Platforms published an article on AT&T's "Cyber Aware" blog about SIM swaps.[43] In the article, AT&T acknowledged that subscribers with "valuable accounts that are accessible online" are likely targets of SIM swaps. AT&T recommended that its customers set up passcodes that would provide "extra security." These passcodes failed to protect Mr. Ross.

81. AT&T therefore knew that its customers' accounts were at risk for *longer than a year* before Mr. Ross' account was breached.

82. AT&T's inadequate security procedures are particularly egregious in light of AT&T's repeated public statements about the importance of cyber security and its public representations about its expertise in this area. AT&T has an entire series on its public YouTube channel ("AT&T ThreatTraq") dedicated to discussing

[42] *Id.* (emphasis added).

[43] Brian Rexroad, "Secure Your Number to Reduce SIM Swap Scams," AT&T's Cyber Aware (Sep. 2017), *available at* https://about.att.com/pages/cyberaware/ni/blog/sim_swap.

and analyzing emerging cybersecurity threats.[44] In its videos, AT&T describes itself as a "network that senses and mitigates cyber threats."[45]

83. AT&T recognizes the risks that arise when a mobile phone is compromised, stating, "Our phones are mini-computers, and with so much personal data on our phones today, it's also important to secure our mobile devices."[46] AT&T's advertisements also stress how central a role mobile phones play in its customer's lives, stating: "My phone is my life" and "My phone is everything." The same ad stresses how the inability to use a mobile phone makes people feel "completely untethered, flailing around."[47]

84. AT&T markets its ability to identify and neutralize emerging cyber threats for its customers. In one video, AT&T employees discuss "threat hunting" – which they describe as "an active threat analysis where you're actually thinking about your adversary."[48] They claim that it's "important" and "something [AT&T has] been doing for a long time."[49] They advise that companies should think about "what would a hacker want to do, where would a hacker go to get my data, what are some of the points on my network that are most vulnerable, or where is the data flow that is potentially going to be a leakage" and state that "having threat hunting as part of a proactive continuous program, integrating with existing security measures, will help [you] stay ahead of the threats."[50] AT&T failed to heed this advice.

---

[44] "AT&T Tech Channel," YouTube, *available at* https://www.youtube.com/user/ATTTechChannel.

[45] "AT&T – Protect Your Network with the Power of &," VIMEO, *available at* https://vimeo.com/172399153.

[46] AT&T, "Mobile Security," YOUTUBE (Feb. 12, 2019), *available* at https://www.youtube.com/watch?v=KSPHS89VnX0.

[47] "AT&T Mobile Movement Campaign – Ads," VIMEO, *available at* https://vimeo.com/224936108.

[48] AT&T Tech Channel, "The Huntin' and Phishin' Episode," YOUTUBE (Apr. 21, 2017), *available at* https://www.youtube.com/watch?v=3g9cPCiFosk.

[49] *Id.*

[50] *Id.*

85. Not only did AT&T advise staying ahead of and addressing cyber threats, it also stressed that these practices could even help identify "insider threats"—*employees within the company or authorized representatives and agents.*

86. In an additional video focused on insider threats, AT&T representatives go on at length about the threat of company insiders selling corporate information *and access*, citing a survey showing that "30% [of respondents] had purposefully sent data outside of their organization at some point in time" and "14% of the people that were interviewed said they would actually sell their corporate log-ins to folks on the outside or sell that data for less than about $250 US."[51] They cited as a "significant concern" the "individuals that have privileged access, that have broad access inside an organization."[52] AT&T therefore knew or should have known that there was a significant risk that its own employees, representatives and agents would provide AT&T customer data—including customer account data—and that the risk was heightened when employees had too broad of access to corporate systems, yet failed to put sufficient systems and resources in place to mitigate that risk, despite its own advice to the contrary.

87. AT&T has also recognized the danger presented to its customers when their email addresses are hacked, as Mr. Ross' was as a result of AT&T's failures. As one AT&T employee puts it: "I think most people do have something valuable [in their email accounts], which is access to all their other accounts, which you can get with a password reset."[53] They call this "something worth keeping safe."[54]

---

[51] AT&T ThreatTraq, "The Real Threat of Insider Threats," YouTube (May 5, 2017), *available at* https://www.youtube.com/watch?v=ZM5tuNiVsjs (emphasis added).
[52] *Id.*
[53] *Id.*
[54] *Id. See also* "Account Hijacking Forum OGusers Hacked", KREBSONSECURITY (May 19, 2019) *at* https://krebsonsecurity.com/2019/05/account-hijacking-forum-ogusers-hacked/

They advised that a "strong, obviously, security awareness program within a company… is extremely important."[55]

88. In this online video series, AT&T makes specific mention of SIM swapping activity. In one video, AT&T's Vice President of Security Platforms (Brian Rexroad) and Principal of Technology Security (Matt Keyser) discuss the hack of a forum called OGusers.[56] In the segment, they discuss the hacking of social media users' account names and point to a news story that highlights—in distinct orange type—that OGusers is a forum popular among people "conducting SIM swapping attacks to seize control over victims' phone numbers."[57]

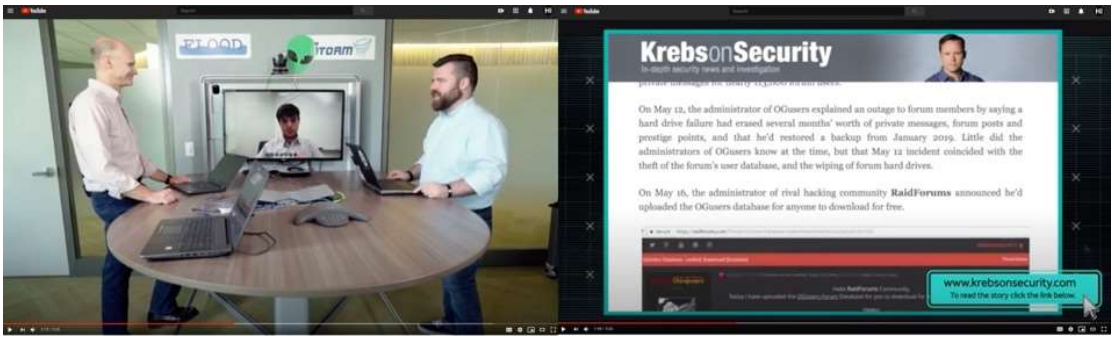


Figure 1

AT&T's Vice President of Security Platforms (Brian Rexroad) and Principal of Technology Security (Matt Keyser) discuss the hack of the "OGusers" forum where Sim swappers meet and a news story highlighting how SIM swappers seize control of victims' phone numbers.

89. AT&T was therefore well aware of the significant risk that AT&T employees, representatives and agents and SIM swapping presented to its customers, and the need to mitigate such risks, but nonetheless failed to take adequate steps to protect Mr. Ross. Instead, it continued to make public statements

[55] *Id.*

[56] AT&T ThreatTraq, "5/31/19 Account-hacking Forum OGusers Hacked," YOUTUBE (May 31 2019), *available at* https://www.youtube.com/watch?time_continue=234&v=cS4xV3cej3A.

[57] *Id.*; *see also* Freeman Indictment at ¶ 2 (Describing how "discussions—such as discussing the manner and means to [SIM swap] attacks generally, and networking among [SIM swap hackers]—typically took place on forums such as "OGusers.").

giving rise to a reasonable expectation that AT&T could—and would—protect its customers.

90. That Mr. Ross was at risk of account breaches at the hands of AT&T employees, representatives and agents is particularly foreseeable—and AT&T's failures are particularly stark—in light of AT&T's history of unauthorized employee, representative and agent access to customer accounts.

91. In 2015, AT&T became subject to an FCC enforcement action, and paid a $25 million civil penalty, for nearly identical failures to protect its customers' sensitive account data.[58] In that case, as AT&T admitted, employees, representatives and agents at an AT&T call center breached 280,000 customers' accounts.[59] Specifically, AT&T employees, representatives and agents had improperly used login credentials to access customer accounts and access customer information that could be used to unlock the customers' devices.[60] The employees then sold the information they obtained from the breaches to a third party.[61]

92. The FCC concluded that AT&T's "failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act."[62]

93. The FCC stressed that the FCA is intended to "ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information."[63] It

---

[58] *In the Matter of AT&T Servs., Inc.*, 30 F.C.C. Rcd. 2808 (2015) at https://docs.fcc.gov/public/attachments/DA-15-399A1.pdf
[59] *Id.* at ¶ 1.
[60] *Id.* at ¶¶ 7, 11.
[61] *Id.* at ¶ 1.
[62] *Id.* at ¶ 2.
[63] *Id.*

stressed its expectation that "telecommunications carriers such as AT&T… take 'every reasonable precaution' to protect their customers' data[.]"[64]

94. As part of its penalty, AT&T entered into a stipulated Consent Decree with the FCC, in which AT&T agreed to develop and implement a compliance plan to ensure appropriate safeguards to protect consumers against similar breaches by improving its privacy and data security practices.[65]

95. This FCC enforcement action underscores AT&T's knowledge of the risk its employees presented to customers, the prevalence of employee breaches to customer data, the sensitive nature of customer CPNI, and its duties to protect and safeguard that data. Nonetheless, more than 3 years after stipulating to the Consent Decree, AT&T still failed to protect its customer from employee breaches of customer CPNI and other account data, virtually identical to the breach at issue here, heightening the degree of its negligence.

96. In January 2020, Princeton researchers released a study finding that top U.S. mobile carriers, including AT&T, do little to protect customers from SIM swap fraud.[66] The study stated "We examined the authentication procedures used by five prepaid wireless carriers when a customer attempted to change their SIM card. ***We found that all five carriers used insecure authentication challenges that could be easily subverted by attackers***. We also found that attackers generally only needed to target the most vulnerable authentication challenges, because the rest could be bypassed." The researchers pretended to be the true phone owner and said they forgot answers to security questions study stating, "Our key finding is that, at the time of our data collection, all 5 carriers used insecure authentication challenges that could easily be subverted by attackers." The study also found: (i)

---

[64] *Id.*

[65] *Id.* at ¶¶ 2, 17-18, 21.

[66] *"An Empirical Study of Wireless Carrier Authentication for SIM Swaps"* Kevin Lee, Ben Kaiser, Jonathan Mayer, Arvind Narayanan Dept of Computer Science and Center for Information Technology Policy, Princeton University, January 10, 2020 at https://www.issms2fasecure.com/assets/sim_swaps-01-10-2020.pdf

Callers only needed to successfully respond to one challenge in order to authenticate, even if they had failed numerous prior challenges. (ii) Four-fifths of SIM-swap fraud attempts were successful, and the researchers attempted 50 SIM swaps and successfully completed 39. (iii) AT&T, Verizon and T-Mobile failed the study. (iv) Some carriers even guided them to the correct answer or didn't ask for anything at all. The Princeton study was widely reported in the media and prompted Congress to get involved. In January 2020, Senator Ron Wyden and 5 other Senators and Congressmen published a letter to FCC Chairman Ajit Pai calling on him to take action to protect consumers against SIM swap fraud, with the Senator stating "SIM swap fraud may also endanger national security. For example, if a cybercriminal or foreign government uses a SIM swap to hack into the email account of a local public safety official, they could then leverage that access to issue emergency alerts using the federal alert and warning system operated by the Federal Emergency Management Agency."[67] Senator Wyden also stated, "Consumers are at the mercy of wireless carriers when it comes to being protected against SIM swaps."[68]

97. According to a Wall Street Journal ("WSJ") article from November 2019, "He Thought His Phone Was Secure; Then He Lost $24 Million to Hackers," investigators say they know of more than 3,000 SIM swap victims, accounting for at least $70 million in theft nationwide (the real numbers are likely much higher considering that many cases go unreported).[69] The WSJ article states, "the people who investigate these attacks consider them some of the most harmful they have ever seen." [69] Victims include high profile public officials, celebrities, and business executives like Jack Dorsey, the CEO of Twitter, whose 2019 SIM swap hack was profiled in the Forbes article "Why Twitter Blames AT&T For The Hack Of Its

[67] https://docs.fcc.gov/public/attachments/DOC-362599A1.pdf
[68] https://twitter.com/ronwyden/status/1215757690875600896
[69] https://www.wsj.com/articles/he-thought-his-phone-was-secure-then-he-lost-24-million-to-hackers-11573221600.

CEO Jack Dorsey Account, Sending Shocking Racist Tweets," and quotes Jeb Su, a Principal Analyst at Atherton Research as saying "*AT&T's poor security policy made this malicious [SIM swap] hack possible.*" [70] The same hacker who executed Jack Dorsey's SIM swap also successfully hacked the District Attorney prosecuting the hacker who AT&T gave control to Mr. Ross' phone service.[71]

98. The SIM swap problem is exacerbated by AT&T's sprawling, mismanaged and problematic call center system. In 2017, AT&T's parent (AT&T, Inc.) had 254,000 employees[72] and 38 third-party call centers across eight non-US countries.[73] A study by the Communication Workers of America ("CWA") entitled "AT&T 2018 Jobs Report: Telecom Giant Hollows Out Middle Class Workforce and Outsources to Global Contractors, Even as it Reaps Tax Windfall" details how AT&T's call center operation is fundamentally broken. Among the key findings were that (i) employees at AT&T vendor call centers face inadequate training and intense pressure to reach unrealistic quotas – making it difficult to meet customer's needs; (ii) overseas vendors, paid as little as $1.60 per hour and often rely on other members of their household to make ends meet, provide inaccurate information, fail to solve problems, offer credits or promotions that cannot be honored, and enroll customers in services they did not request; and (iii) the problems caused by overseas operations add to the burden of U.S. based workers, thereby affecting their work. On information and belief, all of AT&T's numerous customer service representatives are authorized to perform SIM swaps, exacerbating the problem. In order to address its organizational failings, AT&T

---

[70] https://www.forbes.com/sites/jeanbaptiste/2019/08/31/why-twitter-blames-att-for-ceo-jack-dorsey-account-hack-sending-shocking-racist-tweets/.

[71] *"Authorities Arrest Alleged Member of Group That Hacked Jack Dorsey*", Vice by Joseph Cox, November 23, 2019 at https://www.vice.com/en_us/article/gyzawx/authorities-arrest-suspected-jack-dorsey-hacker.

[72] https://www.statista.com/statistics/220683/number-of-atundt-employees-since-2007/

[73] New Report Pulls Back the Curtain on AT&T's Vast Network of Offshored Call Centers at https://cwa-union.org/news/releases/new-report-pulls-back-curtain-on-atts-vast-network-of-offshored-call-centers

could have created a call center dedicated to SIM swaps, and properly vetted, trained and supervised SIM swap customer service representatives, in order to address the problem of unauthorized SIM swaps.

99. Further compounding AT&T's problem-ridden call center and SIM swap mess is how AT&T apparently implemented completely inconsistent authentication protocols at their wholly-owned call centers as compared to their third-party call centers (such as One Touch Direct). An AT&T employee named Robin told Mr. Ross on August 19, 2020 (when Mr. Ross called in via AT&T's "611" feature from his phone, which apparently is routed to an AT&T wholly owned call center) that at the time of the fraudulent SIM swap executed against him (at the AT&T third-party call center One Touch Direct), callers requesting a SIM swap to a customer service representative at an AT&T wholly-owned call center received a text confirmation code that the caller needed to provide to the AT&T customer service representative to complete the SIM swap, whereas customers routed to an AT&T third-party call centers (such as One Touch Direct) did not have receive such a text confirmation, and this was because AT&T did not deploy this simple security confirmation solution to callers routed to AT&T third-party call centers. Indeed, the AT&T employee Robin confirmed to Mr. Ross that on the date of the unauthorized SIM swap, AT&T did ***not*** send a text confirmation to Mr. Ross and Robin also told Mr. Ross that the AT&T representative Ryan S made a note of that in Mr. Ross' customer record on the day of the unauthorized SIM swap.

100. More significantly, for many years AT&T has been fully aware of well-established technology solutions to deter and prevent unauthorized SIM swaps and resulting thefts, which it could easily have implemented well *before* Mr. Ross' phone was SIM swapped, but failed and refused to implement:

a. *Location detection*. At the exact moment of the SIM swap request, AT&T knew the hacker's phone was in New York City (as detailed in the

location data AT&T provided to REACT)[7] and that Mr. Ross' phone was simultaneously in San Francisco, as AT&T tracks customers' location and even sells their location data.[74] AT&T knew that Mr. Ross and his phone could not simultaneously be in both San Francisco and New York City, and could have easily recognized the SIM swap request as a fraud attempt, denied it, and alerted Mr. Ross. AT&T was actually profiting off customers' location data at the same time as it did nothing to use the same location data to prevent the unauthorized SIM swap.

b. *Text message*. AT&T could have simply sent Mr. Ross a text message asking him to confirm whether he requested the SIM swap. He would have replied "no" and AT&T would have then denied the hacker's SIM swap request and could have reported the fraud attempt to Mr. Ross. Banks regularly text customers in this way to confirm even small, low-risk transactions to prevent fraud, as in the text Mr. Ross received from Bank of America confirming $1 transactions in Figure 2.

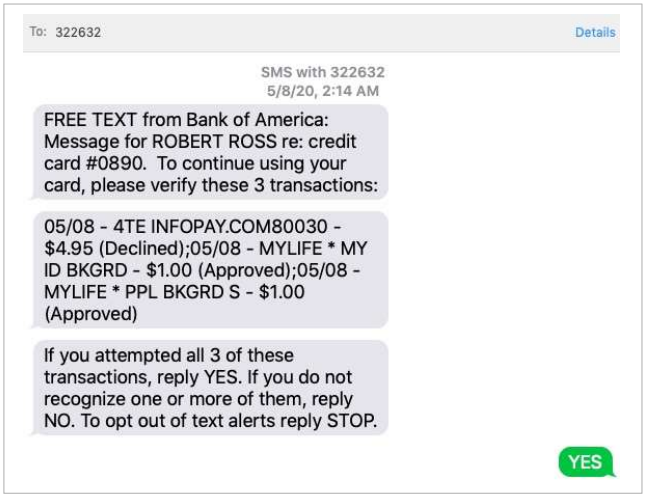


Figure 2

A text message from Bank of America to Mr. Ross asking him to confirm

[74] FCC Proposes Over $200 Million in Fines Against Four Largest Wireless Carriers For Apparently Failing to Adequately Protect Consumer Location Data February 28, 2020 at https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf

$1 transactions, for the purpose of preventing even low-risk transactions.

AT&T regularly sends text messages to its customers for marketing purposes, and asks customers to reply if they want to stop receiving such texts, as in the message AT&T sent to Mr. Ross in Figure 3.

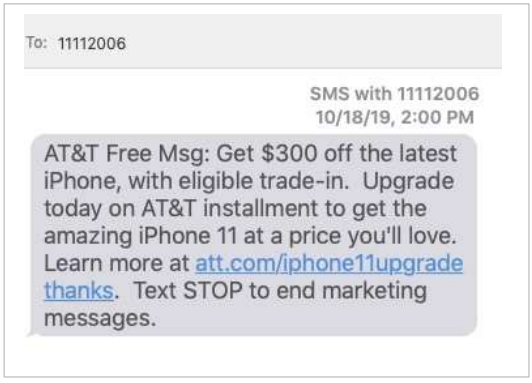


Figure 3

A text message from AT&T to Mr. Ross promoting $300 off the latest iPhone in exchange for an installment upgrade to AT&T's service.

AT&T obviously has the ability to send such simple text messages to its customers requesting a reply. As a direct result of the theft of his life savings due to the SIM swap facilitated by AT&T, Mr. Ross eventually had to cancel his Comcast Xfinity cable TV service, as he could no longer afford it. During Mr. Ross' call with Comcast to request the cancellation, Comcast sent a text confirmation with a web link that required him to reconfirm the request as displayed in Figure 4.

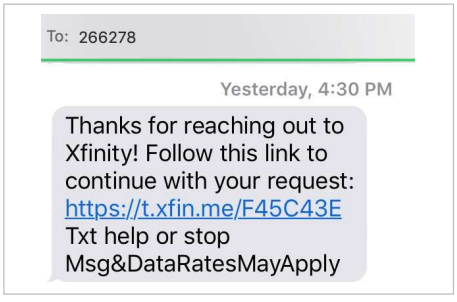


Figure 4

Text from Comcast confirming Mr. Ross' request to cancel his service

Comcast is a direct competitor to AT&T Mobility, as Comcast launched its wireless service branded as Xfinity Mobile, using Verizon's network in 2017[75]. With every text confirmation Mr. Ross now receives such as from Bank of America, Comcast and others, he re-lives and is reminded of the theft as it would have been so easy for AT&T to have avoided destroying his life, with a simple text message.,

c. *Email confirmation.* AT&T could have simply sent Mr. Ross an email asking him to confirm whether he requested the SIM swap. AT&T could have asked for a confirmation directly within the email or directed him to a legitimate link to confirm the request. Mr. Ross would have replied "no" and AT&T would have then denied the hacker's SIM swap request and could have reported the fraud attempt to Mr. Ross.

d. *IMEI detection*. AT&T detects when the same phone has been used in prior unauthorized SIM swaps, and their records (as provided to REACT) show that, prior to the unauthorized SIM swap AT&T facilitated against Mr. Ross, the same device as identified by its IMEI was used in 11 previous unauthorized SIM swaps.[7] AT&T could simply have denied the ability for the phone that was used in previous unauthorized SIM swaps to be used in subsequent SIM swaps, including Mr. Ross', and also could have alerted Mr. Ross to the fraud attempt.

e. *Voice biometrics*. Voice biometrics (or "Voice Id") is a well-established and cost-effective technology that has been implemented by leading financial institutions (e.g., Chase, Wells Fargo and Schwab) to prevent fraud by verifying customers' identities by comparing a caller's voice to a customer (or fraudster) voiceprint stored on file.[76] The technology has also been implemented by

[75] Xfiinity Mobile at https://corporate.comcast.com/company/xfinity/mobile and https://corporate.comcast.com/company/xfinity/mobile

[76] Chase at https://www.chase.com/personal/voice-biometrics, Wells Fargo at https://www.wellsfargo.com/privacy-security/voice-verification, and Schwab at https://www.schwab.com/voice-id.

in Europe, including by the largest carrier in Europe, Deutsche Telekom.[77] While AT&T developed its own voice biometrics solution called AT&T Watson, the technology was never implemented to prevent SIM swaps, and instead was sold to Interactions Corporation ("Interactions") in 2014 in exchange for an equity stake.[78] Ironically, Interactions continues to promote its voice biometrics solution as "Secure and Convenient Authentication,"[79] continues to publicly promote the solution to its large corporate customers who have their own call centers (e.g., banks, insurance companies), publishing a research report entitled "4 emerging technologies that could transform your contact center," which provides in relevant part as follows:Even as companies take steps to guard their IT environments against a growing barrage of cyberthreats, many are neglecting another vulnerable area: their contact centers.

> Social engineering calls to contact centers — in which fraudsters pose as customers and try to trick agents into revealing confidential customer information — are on the rise, according to industry experts, particularly at financial institutions, insurance companies and other businesses that store sensitive data.
>
> Voice biometrics can help your agents know exactly with whom they're talking when they answer a customer call. This technology can recognize voice characteristics passively and verify callers in real time, whether they need to speak to one of your representatives or are using your interactive voice response system.
>
> "By comparing your callers' voiceprints against a database of known fraudster voiceprints, voice biometrics

[77] *Deutsche Telekom turns to biometrics for authentication and fraud detection* https://telecoms.com/491915/dt-turns-to-biometrics-for-authentication-and-fraud-detection/

[78] *AT&T and Interactions Agree to Strategic Transaction in Speech and Multi-Modal Technology Arena* November 5, 2014. https://about.att.com/story/att_and_interactions_agree_to_strategic_transaction_in_speech_and_multi_modal_technology_arena.html

[79] https://www.interactions.com/products/voice-biometrics/

programs can help you identify and track potential thieves before they steal your data."[80]

f. *Data sharing*. Mobile phone carriers in other countries have implemented a "data sharing" solution to prevent theft once an unauthorized SIM swap has occurred. In essence, the carriers allow financial institutions real-time access to their SIM swap data so that the institution can block a requested currency transfer if there has been a SIM swap within a specified time frame (e.g., within 48 hours of the transfer request), since very recent SIM swap combined with a withdrawal request is a strong indicator of fraud. The data sharing solution is widely known and broadly used by major carriers outside of the US. Wired magazine published an article entitled "The SIM Swap Fix That the US isn't Using," which states in relevant part that "While foreign phone carriers are sharing data to stop SIM swap fraud, US carriers are dragging feet."[81] Wired describes that even carriers in developing countries such as Mozambique implemented the solution within a few months of understanding the extent of the problem, and that the Head of IT, Cyber Security & Core Data Networks at Vodacom reported that "[the solution] reduced their SIM swap fraud to nearly zero overnight".[82] Third party aggregators such as Prove.com (formerly Payfone, Inc.) and TeleSign Corporation, who license SIM swap data from non-US carriers and sell it as a fraud prevention offering to banks. Figure 5 shows how all four major carriers in the United Kingdom ("UK"), including British Telecom, Vodafone, O2 and Three, provide their SIM swap data to Prove.com, which in turn sells a fraud prevention

---

[80] "*4 Emerging Technologies That Could Transform Your Contact Center" Mike Rajich, AT&T Director of Contact Center and Enterprise Routing Product Management, AT&T* https://www.business.att.com/learn/research-reports/4-emerging-technologies-that-could-transform-your-contact-center.html

[81] *The SIM Swap Fix That the US Isn't Using, Wired*, Andy Greenberg, April 26, 2019 https://www.wired.com/story/sim-swap-fix-carriers-banks/.

[82] Id.

service to banks enabling them to do real-time SIM swap checks to at the time of customers' high-risk transactions.[83]

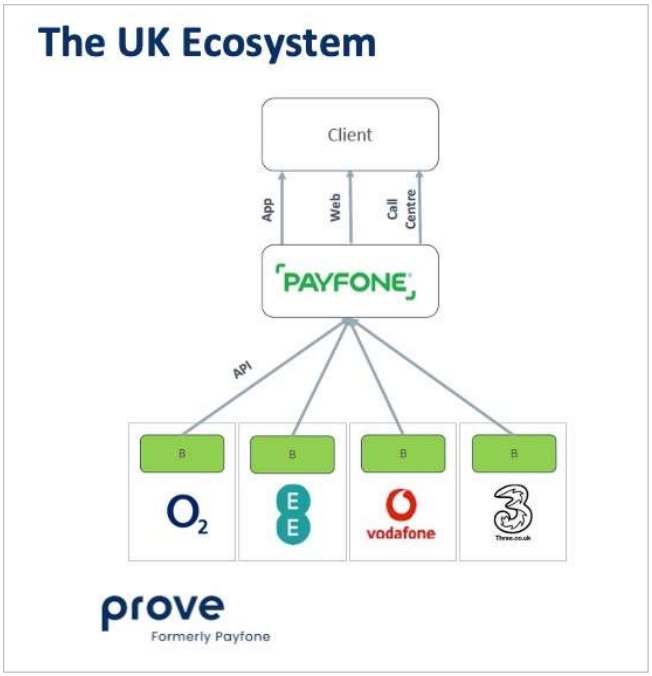


Figure 5

Prove.com system for aggregating SIM swap data from the top 4 UK carriers and enabling clients, such as banks, to perform real-time SIM swap checks

101. Had AT&T implemented any of the foregoing low cost and easy to implement technology solutions, Mr. Ross would not have been the victim of an unauthorized SIM swap.

102. Instead of implementing solutions to ***prevent*** unauthorized SIM swaps, AT&T appears to have made the conscious business decision to profit from unauthorized SIM swaps ***after*** they have occurred. On September 18, 2018, six weeks before Mr. Ross' SIM swap, AT&T, Verizon and T Mobile publicly

[83] https://info.prove.com/psd2-sca-uk-mobile-authentication

announced the joint business scheme they had been developing for months called "Project Verify," now known as ZenKey, to profit from the SIM swap problem. [84]

103. ZenKey is marketed to consumers as an easier and more secure way to log into other online services, stating "Your carrier has a unique ability to identify and protect your mobile identity" and that ZenKey checks for suspicious activity at the carrier (Figure 6), denoting a real-time SIM swap check (as this is the most significant suspicious activity that can occur in a customer's mobile account).[85]

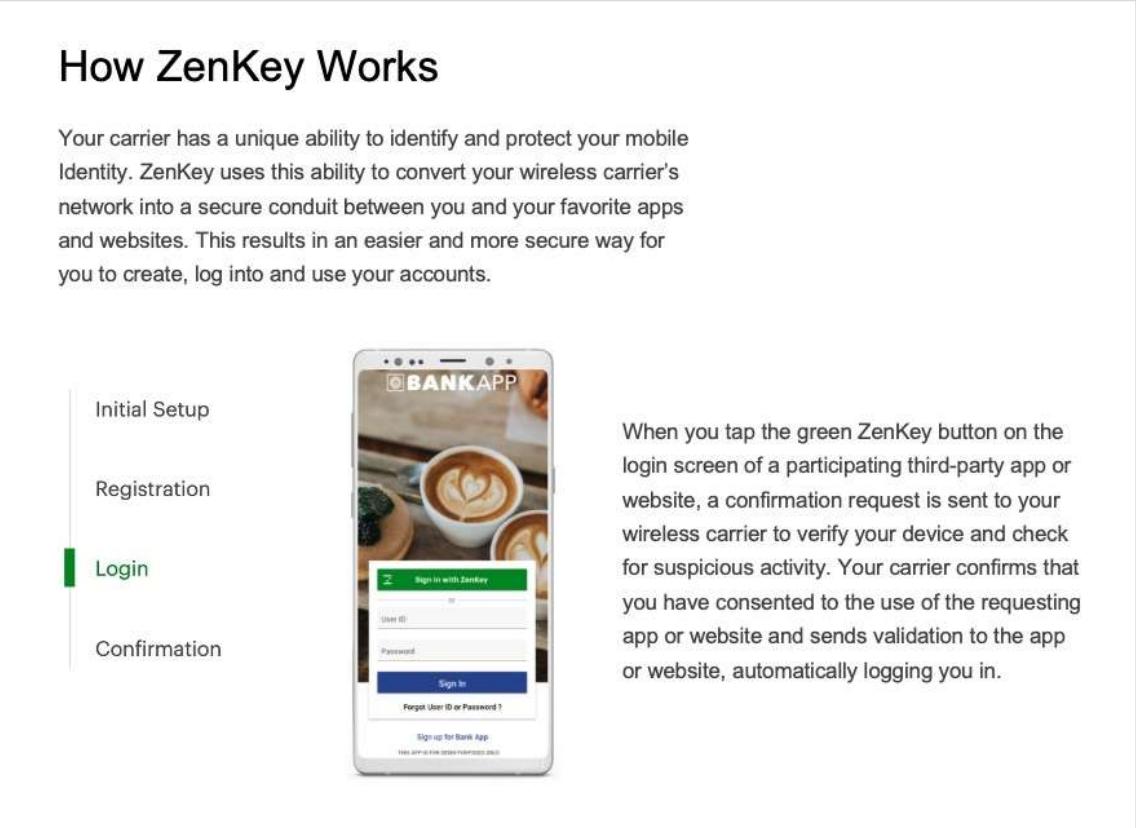


Figure 6

AT&T/ZenKey promotes that it "has a unique ability to identify and protect your mobile identity" and checks for suspicious activity.

[84] *U.S. Mobile Giants Want to be Your Online Identity* at https://krebsonsecurity.com/tag/project-verify/

[85] https://myzenkey.com/how-it-works/

AT&T's ZenKey consumer app is available to consumers currently in the Apple and Google app stores for iPhone and Android devices, as shown in Figure 7.[86]

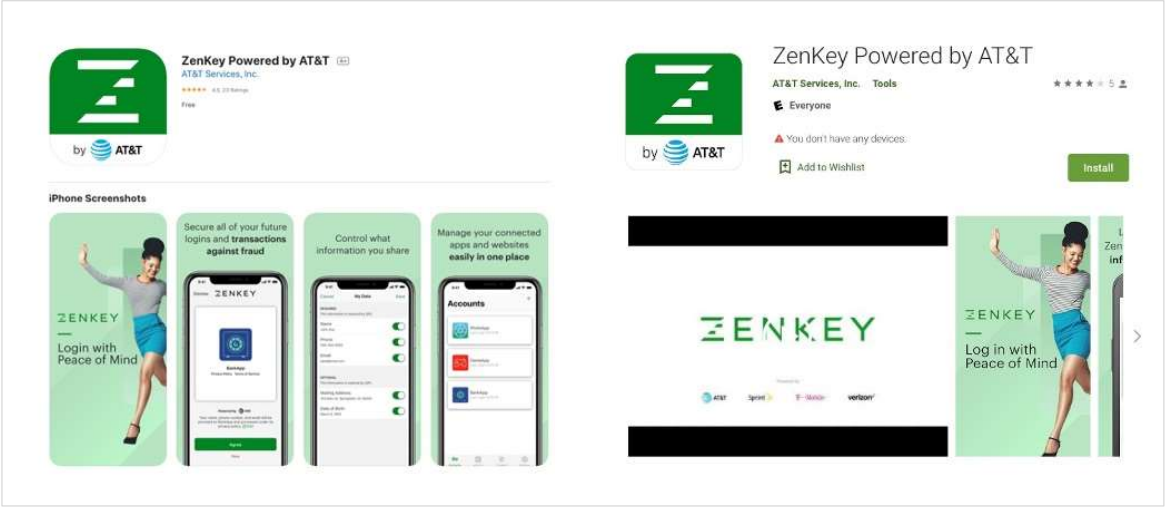


Figure 7

AT&T ZenKey apps for iPhone and Android

At the same time, ZenKey is marketed to financial institutions as an identity and authentication scheme through its "Trust Services" offering, to prevent fraud, with the clear representation that its purpose is to combat SIM swap fraud: "SIM Swap Fraud has already cost businesses hundreds of millions of dollars and the threat is increasing. With ZenKey, fraudsters can no longer access your users' accounts based on stolen credentials and a simple SIM Swap."[87] ZenKey's benefits page states "SIM swap fraud is on the rise and has cost businesses hundreds of millions of dollars ZenKey offers a suite of APIs and event alerts (Trust Services) for Service Providers to receive on-demand fraud signals and automatic indicators."[88] The ZenKey Trust Services proposal, as shown in Figure 8 is effectively executing the same type of real-time SIM swap database check as the data sharing method as described above.

[86] iPhone app at https://apps.apple.com/us/app/zenkey-powered-by-at-t/id1490293601, Android app at https://play.google.com/store/apps/details?id=com.att.cso.consumer.MKapp&hl=en_US

[87] https://myzenkey.com/trust-services/

[88] https://myzenkey.com/business-benefits/

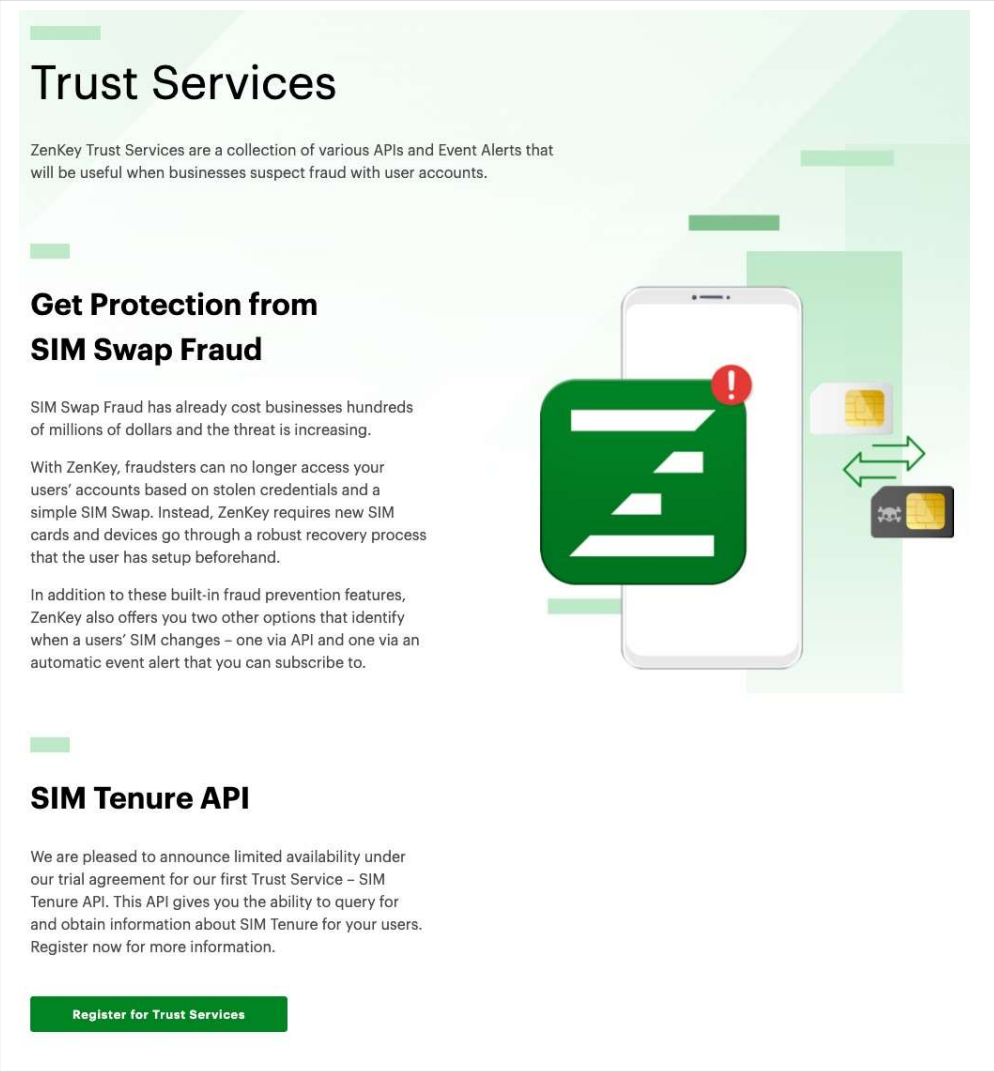


Figure 8

ZenKey's "Trust Services" offering for financial institutions

ZenKey seeks to charge fees to financial institutions in exchange for doing real-time checks against carrier databases to verify when a SIM swap (authorized or not) was last done,[89] and its Portal Agreement Terms of Service provides that "Certain services accessed or available through the [ZenKey] Portal, especially services for which You [e.g. a bank] are asked to subscribe or pay money, may have their own terms and conditions, including but not limited to the Service

[89] ZenKey website at https://myzenkey.com/trust-services/

Agreement."[90] ***ZenKey has failed to date in the marketplace, and has not yet been adopted by financial institutions.***

104. By not implementing even basic solutions to mitigate, let alone substantially reduce SIM swap fraud, AT&T maintains a larger revenue opportunity for ZenKey, as more unauthorized SIM swaps lead to more fraud at banks, which result in a greater need for banks to pay for and check SIM swap data in real-time. While ZenKey has failed to date in the marketplace, and has not yet been adopted by financial institutions, AT&T and its ZenKey partner-competitors continue to invest in it (to date, they have invested around $200 million), promote it and develop it, rather than implement simple solutions to broadly prevent unauthorized SIM swaps.

105. Rather than having easily and expeditiously implemented a data sharing solution in which AT&T licensed their SIM swap database to third party aggregators (such as Prove.com[91] or TeleSign Corporation[92]) or directly to financial institutions (such as Coinbase or Gemini), to enable them to do real-time database checks at the time of a high-risk transactions (as non-US carriers do[81]), AT&T focused its efforts developing ZenKey in collusion with Verizon and T-Mobile in their ill-conceived (and to-date failed) attempt to more directly profit and control the authentication market opportunity.

F. Defendants Are Liable for the Acts of Their Employees, Representatives and Agents

106. Defendants are liable for the acts of their employees, representatives and agents who facilitated the unauthorized access to, and resulting theft from, Mr. Ross.

---

[90] https://portal.myzenkey.com/terms

[91] *The End of Dangerous SIM Swap Fraud is Here: Payfone Extends Real-Time SIM Swap Detection Algorithms* at https://www.payfone.com/press/the-end-of-dangerous-sim-swap-fraud-is-here/

[92] How TeleSign Protects Transactions from SIM Swap Fraud at https://www.telesign.com/blog/how-telesign-protects-transactions-from-sim-swap-fraud

107. Defendants failed to put in place adequate systems and procedures to prevent the unauthorized employee, representative and agent access to Mr. Ross' account and related data. Defendants failed to properly hire and supervise their employees, representatives and agents, allowing them to access Mr. Ross' sensitive and confidential account data without his authorization and provide that data to third parties.

108. In the context of AT&T's enterprise as a telecommunications carrier, an employee, representative and agent accessing a customer's account information and effectuating a SIM swap—even without authorization—is not so unusual or startling that it would be unfair to include the loss resulting from such unauthorized access among other costs of AT&T's business – particularly in light of AT&T's awareness of the risk of SIM swaps to its customers.

109. Further, imposing significant liability on AT&T and its agents may prevent recurrence of SIM swap behavior because it creates a strong incentive for vigilance and proper safeguarding of customers' data by AT&T—which, in the case of its customers, is the sole party in the position to guard substantially against this activity, as it is the custodian and guardian of this data.

110. As a customer of AT&T, Mr. Ross is entitled to rely upon the presumption that AT&T and the employees, representative and agents entrusted with the performance of AT&T's business have faithfully and honestly discharged the duty owed to him by AT&T, and that they would not gain unauthorized access to his account.

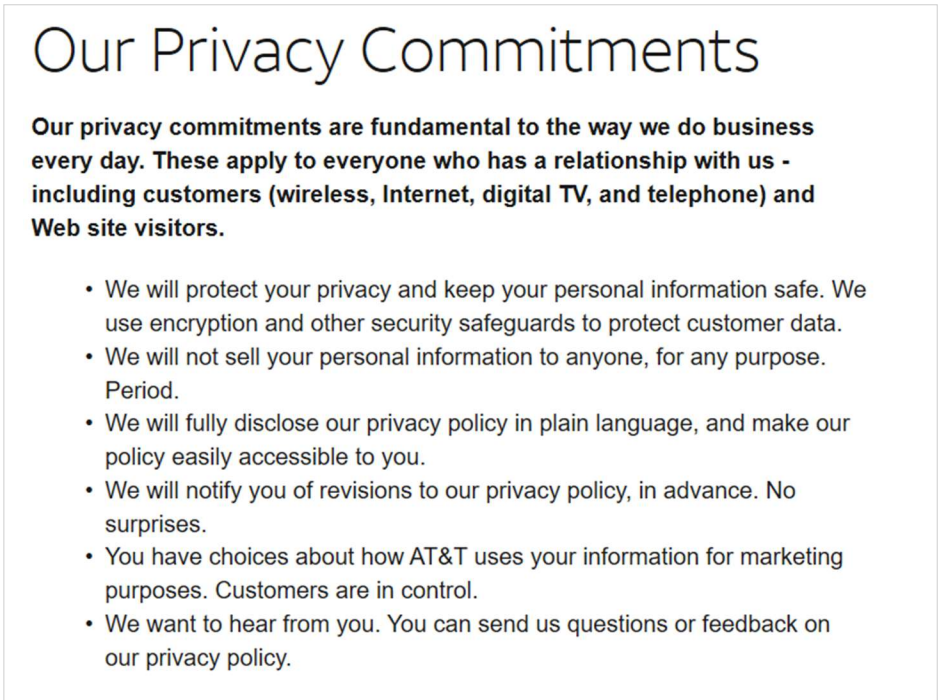
111. The reasonableness of Mr. Ross' expectations that AT&T would safeguard his data is confirmed by the fact that the federal agency responsible for overseeing AT&T's duties to its customers, the FCC, has stated that it "fully

expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[93]

AT&T's Misrepresentations and Omissions.

112. AT&T's Privacy Policy, and the "Privacy Commitments" included therein, falsely represents and fails to disclose material information about its data security practices.

113. In its Privacy Policy, AT&T promised to protect Mr. Ross' privacy and personal information, including by using "security safeguards." AT&T further pledges that it will not sell customer data. These representations created an expectation that Mr. Ross' AT&T account and associated data would be safe and secure, that employees, representatives and agents would not access his account without authorization, that his data would be protected from unauthorized disclosure, and that he could control how and when his data was accessed. Figure 9, immediately below, is an excerpt from AT&T's Privacy Policy.



Our Privacy Commitments

Our privacy commitments are fundamental to the way we do business every day. These apply to everyone who has a relationship with us - including customers (wireless, Internet, digital TV, and telephone) and Web site visitors.

- We will protect your privacy and keep your personal information safe. We use encryption and other security safeguards to protect customer data.
- We will not sell your personal information to anyone, for any purpose. Period.
- We will fully disclose our privacy policy in plain language, and make our policy easily accessible to you.
- We will notify you of revisions to our privacy policy, in advance. No surprises.
- You have choices about how AT&T uses your information for marketing purposes. Customers are in control.
- We want to hear from you. You can send us questions or feedback on our privacy policy.

Figure *9* [94]

[93] 2007 CPNI Order ¶ 64.
[94] "Privacy Policy," AT&T, attached hereto as Exhibit C.

114. AT&T's representation that it "uses encryption and other security safeguards to protect customer data" is false and extremely misleading.

115. As alleged fully above, AT&T allowed its employees, representatives and agents to access Mr. Ross' account, and the CPNI and other sensitive data contained therein, without his authorization. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation.

116. Upon information and belief, AT&T's security safeguards were inadequate, including its system which—upon information and belief—allowed an individual employee, representative and agent to conduct SIM swaps without adequate technical safeguards and oversight, even when that employee, representative and agent authorizes a COAM SIM swap over the phone in violation of company policy.

117. "Having one employee who can conduct these SIM swaps without any kind of oversight seems to be the real problem," says Lieutenant John Rose, a member of the California-based Regional Enforcement Allied Computer Team ("REACT"), a multi-jurisdictional law enforcement partnership specializing in cybercrime.67F[95] "And it seems like [the carriers] could really put a stop to it if there were more checks and balances to prevent that. It's still very, very easy to SIM swap, and something has to be done because it's just too simple. Someone needs to light a fire under some folks to get these protections put in place."

118. AT&T failed to put in place adequate systems and procedures to prevent the unauthorized employee, representative and agent access to and take over of Mr. Ross' account and related data. In connection with subsequent criminal investigations into Mr. Ross' SIM swap, AT&T informed law enforcement that it had the capacity to see how many different SIM cards had been associated with the

[95] Busting SIM Swappers and SIM Swap Myths," KREBSONSECURITY (Nov. 18, 2018), *available at* https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths.

same single mobile phone's IMEI.[96] In other words, AT&T could see when one mobile phone had multiple SIM cards associated with it in a short amount of time.[97]

119. AT&T also informed law enforcement that the hacker involved in Mr. Ross' SIM swap had requested that *eleven different phone numbers* be moved onto his phone (identified by its IMEI number) in the twenty-one days before Mr. Ross' swap.[98] The hacker sometimes moved three different AT&T numbers onto the same phone *in a single day*.[99] AT&T certainly had the capability to see this behavior, and could and should have flagged it as suspicious. If AT&T had proper security safeguards in place, it would have recognized this behavior, flagged it as suspicious, and prevented any further SIM swaps onto that phone – thereby protecting Mr. Ross.

120. Additionally, as alleged fully above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Ross' data was accessed and provided to third parties. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation. AT&T easily and very quickly detected that the same phone was used in eleven prior unauthorized SIM swaps *before* the unauthorized SIM swap on Mr. Ross' phone, and gave this information to the REACT cybercrime task force.[7] However, AT&T did nothing to stop the hacker from using the same phone for multiple unauthorized SIM swaps, and had no voice biometric system or other solution in place to prevent the unauthorized SIM swaps.

121. AT&T's representation that it "will protect [customers'] privacy and keep [their] personal information safe" is false and misleading.

122. As alleged fully above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Ross' account and the data therein

---

[96] Ex. B. at pp. 8, 22.
[97] *Id.*
[98] *Id.*
[99] *Id.* at 22.

were accessed and used without his authorization or consent and disclosed to third parties. Mr. Ross' privacy and personal information was not safe, as demonstrated by the breach of his AT&T account. AT&T's statement that it would protect customers' privacy and keep their personal information safe is therefore a material misrepresentation.

123. AT&T also makes numerous false or misleading representations concerning its treatment of customers' data that qualifies as CPNI under the FCA.

124. AT&T explicitly and falsely represents in its Privacy Policy that it does not "sell, trade or share" their CPNI:

> We do not sell, trade or share your CPNI with anyone outside of the AT&T family of companies* or our authorized agents, unless required by law (example: a court order).[100]

125. As alleged fully above, AT&T and its employees, representatives and agents provided access to Mr. Ross' CPNI to third-party hackers. This use was not required by law and was instead *prohibited* by law.

126. AT&T also states that it only uses CPNI "internally" and its *only* disclosed use of CPNI is "among the AT&T companies and our agents in order to offer you new or enhanced services."[101]

127. Defendants' employees', representatives' and agents' use of Mr. Ross' account and related data as described herein was not for "internal" AT&T purposes, nor was it used to market AT&T services. AT&T's statements regarding the use of customer CPNI are therefore material misrepresentations. Its failure to disclose this is a material omission.

---

[100] "Customer Proprietary Network Information (CPNI)," AT&T, Ex. C at 31-32. The "AT&T family of companies" is defined as "those companies that provide voice, video and broadband-related products and/or services domestically and internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services." *Id.*

[101] *Id.*

128. AT&T also falsely represents that it "uses technology and security features, and strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI."

129. As alleged fully above, AT&T and its agents failed to safeguard Mr. Ross' CPNI. Instead, it stored customer CPNI in such a way that unauthorized access was easily obtained by employees and third parties. AT&T's statements regarding the technology and security features it uses to safeguard customer CPNI are therefore material misrepresentations.

130. AT&T was obligated to disclose the weaknesses and failures of its account and data security practices, as AT&T had exclusive knowledge of material facts not known or knowable to its customers, AT&T actively concealed these material facts from Mr. Ross, and such disclosures were necessary to materially qualify its representations that it took measures to protect consumer data and to materially qualify its partial disclosures concerning its use of customers' CPNI. Further, AT&T was obligated to disclose its practices under the FCA.

131. A reasonable person would be deceived and misled by AT&T's misrepresentations, which clearly indicated that AT&T would safeguard its customers' personal information and CPNI.

132. AT&T intentionally misled Mr. Ross regarding its data security practices in order to maintain his business, make money from his account, and evade prosecution for its unlawful acts. Furthermore, AT&T has invested millions into ZenKey to profit from the SIM swap problem, thereby incentivizing itself (and its two primary competitors) to not timely solve the problem to protect its customers, for which other carriers have implemented highly effective solutions.

133. AT&T's representations that it protected customers' personal information, when in fact it did not, were false, deceptive, and misleading and therefore a violation of the FCA.

VI. CLAIMS FOR RELIEF

COUNT I
Violations of The Federal Communications Act, 47 U.S.C. § 201 *et seq.*

134. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

135. Defendants have violated 47 U.S.C. § 222(a) by failing to protect the confidentiality of Mr. Ross' CPNI, as detailed herein.

136. Defendants have violated 47 U.S.C. § 222(c) by using, disclosing, and/or permitting access to Mr. Ross' CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein. Defendants also caused and/or permitted third parties to use, disclose, and/or permit access to Mr. Ross' CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein.

137. As fully alleged above, Mr. Ross has suffered injury to his person, property, health, and reputation as a consequence of Defendants' violations of the FCA. Additionally, Mr. Ross has suffered emotional damages, including severe anxiety and depression, mental anguish, and suffering as a result of Defendants' acts and practices. These emotional damages have led directly to physical issues; for example, Mr. Ross began stress-eating which resulted in Mr. Ross gaining approximately 40 pounds in only a few months following the Defendants-facilitated thefts.

138. Mr. Ross seeks the full amount of damages sustained as a consequence of Defendants' violations of the FCA, together with reasonable attorneys' fees, to be fixed by the Court and taxed and collected as part of the costs of the case. Mr. Ross also moves for a writ of injunction or other proper process, mandatory or otherwise, to restrain Defendants and their officers, agents, or

representatives from further disobedience of the 2007 and 2013 CPNI Orders, or to compel their obedience to the same.

COUNT II
Violations of The California Unfair Competition Law ("UCL") under the Unlawful, Unfair and Fraudulent Prongs, California Business & Professional Code § 17200 *et seq*.

139. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

140. California's Unfair Competition Law (UCL) prohibits any "unlawful, unfair or fraudulent business act or practice." Defendants' business acts and practices complained of herein were unlawful, unfair, and fraudulent.

141. AT&T made material misrepresentations and omissions concerning its safeguarding of Mr. Ross' CPNI. As alleged fully above, a reasonable person would attach importance to the privacy of his sensitive account data in determining whether to contract with a mobile phone provider.

142. Defendants had a duty to disclose the nature of their inadequate security practices and failures in hiring, training, and supervising staff. Defendants had exclusive knowledge of material facts not known or knowable to AT&T customers and Defendants actively concealed these material facts from customers.

143. Further, additional disclosures were necessary to materially qualify AT&T's representations that it did not sell consumer data and took measures to protect that data, and its partial disclosures concerning its use of customers' CPNI. AT&T was obligated to disclose its practices, as required by the FCA. The magnitude of the harm suffered by Mr. Ross underscores the materiality of AT&T's omissions.

144. A reasonable person, such as Mr. Ross, would be deceived and misled by AT&T's misrepresentations, which indicated that Defendants would safeguard its customers' personal and proprietary information.

145. AT&T intentionally misled its customers regarding its data protection practices in order to attract customers and evade prosecution for its unlawful acts.

146. Defendants' actions detailed herein constitute an unlawful business act or practice. As alleged herein, Defendants' conduct is a violation of the California constitutional right to privacy and the FCA.

147. Defendants' actions detailed herein constitute an unfair business act or practice.

148. Defendants' conduct lacks reasonable and legitimate justification in that Mr. Ross has been misled as to the nature and integrity of AT&T's goods and services and has suffered injury as a result.

149. The gravity of the harm caused by Defendants' practices far outweigh the utility of their conduct. Defendants' practices were contrary to the letter and spirit of the FCA and its corresponding regulations, which require mobile carriers to disclose customers' CPNI only upon proper notice, consent, and authorization, and aims to vest carrier customers with control over their data. Due to the surreptitious nature of Defendants' actions, Mr. Ross could not have reasonably avoided the harms incurred as a result.

150. As the FCA establishes, it is against public policy to allow carrier employees or other third parties to access, use, or disclose telecommunications customers' sensitive account information. The effects of Defendants' conduct are comparable to or the same as a violation of the FCA.

151. Defendants' actions detailed herein constitute a fraudulent business act or practice.

152. As established herein, Mr. Ross has suffered injury in fact and economic harm as a result of AT&T's unfair competition. Additionally, had Defendants disclosed the true nature and extent of their data security and protection practices—and the flaws inherent in their systems—and their unwillingness to

properly protect its customers, Mr. Ross would not have subscribed to or paid as much money for AT&T's mobile services.

153. Mr. Ross seeks injunctive and declaratory relief for Defendants' violations of the UCL. Mr. Ross seeks public injunctive relief against Defendants' unfair and unlawful practices in order to protect the public and restore to the parties in interest money or property taken as a result of Defendants' unfair competition. Mr. Ross seeks a mandatory cessation of Defendants' practices, and proper safeguarding of AT&T account data.

COUNT III
Violations of the California Constitutional Right to Privacy

154. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

155. The California Constitution declares that, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. Art. I, § 1.

156. Mr. Ross has a reasonable expectation of privacy in his mobile device and his AT&T account information.

157. Defendants intentionally intruded on and into Mr. Ross' solitude, seclusion, or private affairs by allowing its employees and third parties to improperly access Mr. Ross' confidential AT&T account information without proper consent or authority.

158. The reasonableness of Mr. Ross' expectations of privacy is supported by AT&T and its agents' unique position to safeguard his account data, including the sensitive and confidential information contained therein, and protect Mr. Ross from SIM swap attacks.

159. AT&T and its agents' intrusions into Mr. Ross' privacy are highly offensive to a reasonable person. This is evidenced by federal legislation enacted

by Congress and rules promulgated and enforcement actions undertaken by the FCC aimed at protecting AT&T customers' sensitive account data from unauthorized use or access.

160. The offensiveness of Defendants' conduct is heightened by AT&T's material misrepresentations to Mr. Ross concerning the safety and security of his account.

161. Mr. Ross suffered great personal and financial harm by the intrusion into his private affairs, as detailed throughout this Complaint.

162. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Mr. Ross. But for Defendants' agents' and employees' unauthorized access to Mr. Ross' account and AT&T's failure to protect Mr. Ross from such harm through adequate security and oversight systems and procedures, Mr. Ross would not have had his personal privacy repeatedly violated and would not have been a victim of SIM swap theft resulting in his loss of $1,000,000 in cash and the breach of sensitive personal information.

163. As a result of Defendants' actions, Mr. Ross seeks nominal and punitive damages in an amount to be determined at trial. Mr. Ross seeks punitive damages because Defendants' actions were malicious, oppressive, and willful. Defendants knew or should have known about the risks faced by Mr. Ross, and the grave consequences of such risks. Nonetheless, Defendants utterly failed to protect Mr. Ross, and instead, AT&T has invested millions of dollars into a scheme to profit from SIM swaps through ZenKey. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT IV
Negligence

164. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

165. Defendants owed a duty to Mr. Ross—arising from the sensitivity of his AT&T account information and the foreseeability of harm to Mr. Ross should Defendants fail to safeguard and protect such data—to exercise reasonable care in safeguarding his sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing AT&T's and its agents', partners', and independent contractors' systems, protocols, and practices to ensure that Mr. Ross' information was adequately secured from unauthorized access.

166. Federal law and regulations, as well as AT&T's privacy policy, acknowledge Defendants' duty to adequately protect Mr. Ross' confidential account information.

167. Defendants owed a duty to Mr. Ross to protect his sensitive account data from unauthorized use, access, or disclosure. This included a duty to ensure that his CPNI was used, accessed, or disclosed only with proper consent.

168. Defendants owed a duty to Mr. Ross to implement a system to safeguard against and detect unauthorized access to Mr. Ross' AT&T data in a timely manner.

169. Defendants owed a duty to Mr. Ross to disclose the material fact that their data security practices were inadequate to safeguard Mr. Ross' AT&T account data from unauthorized access by its own employees and others.

170. AT&T had a special relationship with Mr. Ross due to its status as his telecommunications carrier, which provided an independent duty of care. AT&T had the unique ability to protect its systems and the data it stored thereon from unauthorized access.

171. Mr. Ross' willingness to contract with AT&T, and thereby entrust AT&T with his confidential and sensitive account data, was predicated on the understanding that AT&T and its agents would undertake adequate security and consent precautions.

172. Defendants breached their duties by, *inter alia*: (a) failing to implement and maintain adequate security practices to safeguard Mr. Ross' AT&T account and data—including his CPNI—from unauthorized access, as detailed herein; (b) failing to detect unauthorized accesses in a timely manner; (c) failing to disclose that their data security practices were inadequate to safeguard Mr. Ross' data; (d) failing to supervise their agents and employees and prevent them from accessing and utilizing Mr. Ross' AT&T account and data without authorization; and (e) failing to provide adequate and timely notice of unauthorized access.

173. Defendants were also negligent in their authorization of Mr. Ross' SIM card swap. Defendants knew or should have known that at least ten different AT&T numbers had been moved to the same mobile phone (identified by its IMEI) in the weeks leading up to Mr. Ross' SIM swap. Defendants knew or should have known that this was highly suspicious. Nevertheless, Defendants effectuated the transfer of Mr. Ross' AT&T account to this same mobile phone. Defendants had the technical capacity to track this behavior—as reflected in its willingness to do so quickly for law enforcement—but nonetheless failed to utilize it for the benefit and protection of Mr. Ross.

174. But for Defendants' breaches of their duties, Mr. Ross' data would not have been accessed by unauthorized individuals.

175. Mr. Ross was a foreseeable victim of Defendants' inadequate data security practices and consent mechanisms. As alleged fully above, AT&T and its agents knew or should have known that SIM swaps presented a serious threat to its customers, including Mr. Ross, before Mr. Ross' account was breached for the first time. Defendants also knew or should have known that improper procedures and systems to safeguard customer data could allow their agents and employees to authorize customers' accounts and data, as occurred in the 2015 FCC enforcement action.

176. Defendants knew or should have known that unauthorized access would cause damage to Mr. Ross. AT&T admitted that unauthorized account access presents a significant threat to its customers, and it became aware during its 2015 FCC enforcement action of the harms caused by unauthorized account access.

177. Defendants' negligent conduct provided a means for unauthorized individuals to access Mr. Ross' AT&T account data, take over control of his mobile phone, and use such access to hack into numerous online accounts in order to rob Mr. Ross and steal his personal information. As a result of Defendants' failure to prevent unauthorized accesses, Mr. Ross suffered grave injury, as alleged fully above, including severe emotional distress. This emotional distress arose out of Defendants' breach of their legal duties. The damages Mr. Ross suffered were a proximate, reasonably foreseeable result of Defendants' breaches of their duties. Therefore, Mr. Ross is entitled to damages in an amount to be proven at trial.

178. The injury and harm suffered by Mr. Ross was the reasonably foreseeable result of AT&T's failure to exercise reasonable care in safeguarding and protecting Mr. Ross's Personal Information, including his CPI and CPNI. AT&T's misconduct as alleged herein is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Ross and despicable conduct that has subjected Mr. Ross to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Ross is entitled to punitive damages against AT&T under Civil Code § 3294(a). Mr. Ross further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of AT&T employees in evading or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

COUNT V
Concealment

179. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

180. As alleged above, AT&T, including Chief Security Officer Bill O'Hern and Chief Compliance Officer David S. Huntley, who are respectively in charge of AT&T's security and privacy protections, knew that its data security measures were grossly inadequate, that its employees and agents could readily bypass the procedures, that its employees actively cooperated with hackers and thieves, and that it was incapable of living up to its commitments to consumers, including to Mr. Ross, under state and federal law, as well as under its own Privacy Policy, to protect his Personal Information, including CPI and CPNI.

181. Mr. Ross was unaware that AT&T's security measures did not include low cost and readily available solutions which would have prevented his SIM swap and resulting theft.

182. AT&T, including Mr. O'Hern and Mr. Huntley, knew or should have known from prior incidents and contacts with law enforcement that its system was subject to SIM swap fraud, that its employees cooperated with hackers in such fraud, that such fraud was prevalent in the cryptocurrency community, and that its security measures were ineffective in preventing the fraud. Mr. O'Hern should have been well aware of this because he is in charge of security and AT&T and Mr. Huntley should have known because he is in charge of insuring that AT&T protects the privacy of its customers.

183. AT&T did not disclose these things to Mr. Ross and willfully deceived Mr. Ross by concealing the true facts concerning its data security, which AT&T was legally obligated and had a duty to disclose. It did so in order to induce Mr. Ross to remain as its customer.

184. Had AT&T disclosed the true facts about its dangerously poor data

security practices and that is was motivated to profit from SIM swaps rather than correct the problem, Mr. Ross would have taken further measures to protect himself and would have ceased being a customer of AT&T.

185. Mr. Ross justifiably relied on AT&T to provide accurate and complete information about its data security in continuing to be AT&T's customer. Rather than disclosing the inadequacies in its security, including the additional security it encouraged Mr. Ross to place on his account, AT&T willfully suppressed any information relating to such inadequacies.

186. AT&T's actions are "deceit" under Cal. Civ. Code § 1710 in that they are the suppression of a fact by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact Because of the deceit by AT&T, it is liable under Cal. Civ. Code§ 1709 for "any damage which [Mr. Ross] thereby suffers."

187. Because of this deceit by Defendants, Mr. Ross's Personal Information, including his CPI and CPNI, as described above, was compromised by hackers and he was deprived of $1 million. The connection between AT&T, the SIM swap and the loss of Mr. Ross's funds is alleged hereinabove. In addition, Mr. Ross's Personal Information is now easily available to hackers, including through the Dark Web. Mr. Ross is further damaged to the extent of the amounts that he has paid AT&T for wireless services, because those services were either worth nothing or worth less than was paid for them because of lack of security. Mr. Ross has also suffered substantial out-of-pocket costs because of AT&T's inadequate security.

188. Because AT&T's deceit is fraud under Civil Code § 3294(c)(3) ,and AT&T's conduct was done with malice, fraud and oppression, Mr. Ross is entitled to punitive damages under Civil Code § 3294(a). Mr. Ross further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of

AT&T employees in evading or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

COUNT VI
Negligent Supervision and Entrustment

189. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

190. AT&T conducts its business activities through employees or other agents, including One Touch Direct and One Touch Direct-SA.

191. Defendants are liable for harm resulting from their agents and employees because they were reckless or negligent in employing and/or entrusting agents and employees in work involving the risk of harm to others, including Mr. Ross.

192. On information and belief, Defendants knew or had reason to believe that their agents and employees were unfit and failed to exercise reasonable care in properly investigating and overseeing them. AT&T was negligent in supervising its agents and in entrusting them with what it knew to be highly sensitive confidential information. One Touch Direct and One Touch Direct-SA were negligent in supervising their agents and employees and in entrusting them with what they knew to be highly sensitive confidential information. Defendants knew or had reason to know that their agents and employees were likely to harm others in view of the work AT&T entrusted to them. Specifically, AT&T entrusted its agents and employees with the responsibility to conduct SIM card changes without sufficient oversight – as demonstrated by the representative and agent effectuating the October 2018 SIM swap on Mr. Ross' account despite AT&T's policy disallowing COAM SIM changes over the phone.

193. Additionally, as alleged fully above, the hacker involved in Mr. Ross' SIM swap had associated numerous different SIM cards with the same device IMEI

in the days leading up to Mr. Ross' attack. Despite the highly suspicious nature of this activity, and AT&T's ability to track such requests, AT&T and its agents failed to put any additional protections on customer accounts to prevent its employees from approving additional SIM swaps to the same IMEI.

194. Upon information and belief, Defendants failed to exercise due care in selecting their agents and employees, and thereby negligently or recklessly employed employees to do acts—including accessing customer accounts and effectuating SIM swaps—which necessarily brought them in contact with others, including Mr. Ross, while in the performance of those duties.

195. Defendants' acts, as alleged herein, were negligent in that they created the risk of unauthorized account access, SIM card changes, and the damages resulting therefrom.

196. Defendants also failed to properly supervise their agents and employees, and instead continued to negligently entrust them with sensitive customer data. On information and belief, had AT&T not contracted out customer service functions to third parties such as One Touch Direct and One Touch Direct-SA, and had One Touch Direct or One Touch Direct-SA fired the involved the employee when they first began to exhibit suspicious SIM swap activity—including but not limited to approving SIM changes that violated AT&T policy—Mr. Ross would not have been injured.

197. On information and belief, had Defendants built a system to effectively authenticate and verify consumer consent before allowing its agents or employees to access their CPNI—as required by the FCA—Mr. Ross would not have been injured.

198. On information and belief, had Defendants prevented individual employees from unilaterally performing SIM swaps without proper oversight, Mr. Ross would not have been injured.

199. In sum, Defendants gave their agents and employees the tools and opportunities they needed to gain unauthorized access to Mr. Ross' account and failed to prevent them from doing so, thereby allowing them to use AT&T's systems to perpetuate privacy breaches and thefts against Mr. Ross.

200. The Defendants' agent(s') and employee(s') actions have a causal nexus to their employment. Mr. Ross' injuries arose out of his contract with AT&T as his carrier, and AT&T's access to his CPNI and account data as a result. The risk of injury to Mr. Ross was inherent in the AT&T working environment.

201. Mr. Ross' injury was also foreseeable. As alleged fully above, Defendants were aware of the risks that SIM swaps presented to AT&T customers. Defendants were also aware that AT&T customers' accounts were vulnerable to unauthorized access by their agents and employees, as demonstrated in the 2015 FCC enforcement action. Furthermore, Mr. Ross' injury was foreseeable as Defendants could have and should have seen that the same hacker phone had been used in multiple previous unauthorized SIM swaps.

COUNT VII
Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030

202. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

203. Mr. Ross' mobile device is capable of connecting to the Internet.

204. Defendants' agents and employees, in the scope of their employment, intentionally accessed Mr. Ross' mobile device, and assisted others in accessing his mobile device, without Mr. Ross' authorization, in order to assist hackers in their theft of Mr. Ross.

205. The Defendants agents and employees took these actions knowing that they would cause damage to Mr. Ross' mobile device, as well as damage to the information located on his mobile device.

206. The Defendants agents and employees caused Mr. Ross' mobile device and much of the data on it to be unusable to him.

207. Because of the Defendants' agents' and employees' actions, Mr. Ross suffered damage to his mobile device and damage to information on his mobile device, including being unable to access information and data on his mobile device and being unable to access his personal accounts, including his personal (e.g. Gmail) and financial (e.g. cryptocurrency and PayPal) accounts.

208. The act of swapping Mr. Ross' AT&T mobile SIM card was in the scope of the Defendants' agents and employees' work.

209. Further, Mr. Ross spent in excess of $5,000 investigating who accessed his mobile device and damaged information on it.

VII. PRAYER FOR RELIEF

210. WHEREFORE, Plaintiff Robert Ross requests that judgment be entered against Defendants and that the Court grant the following:

A. Judgment against Defendants for Plaintiff's asserted causes of action;

B. Public injunctive relief requiring cessation of Defendants' acts and practices complained of herein pursuant to, *inter alia*, Cal. Bus. & Prof. Code § 17200 and 47 U.S.C. § 401(b);

C. Pre- and post-judgment interest, as allowed by law;

D. An award of monetary damages, including punitive damages, as allowed by law;

E. Reasonable attorneys' fees and costs reasonably incurred, including but not limited to attorneys' fees and costs pursuant to 47 U.S.C. § 206; and

F. Any and all other and further relief to which Plaintiff may be entitled.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues so triable.

DATED:

CHRISTOPHER GRIVAKES
AFFELD GRIVAKES LLP

By: /s/ DRAFT
Christopher Grivakes

Attorneys for Plaintiff ROBERT ROSS

EXHIBIT A

27

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

-vs-

Case:2:19-cr-20246
Judge: Hood, Denise Page
MJ: Patti, Anthony P.
Filed: 04-18-2019 At 04:44 PM
SEALED MATTER (dat)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER
D-3 COLTON JURISIC
D-4 REYAD GAFAR ABBAS
D-5 GARRETT ENDICOTT
D-6 RYAN STEVENSON

Defendants.
_____/

Vio: 18 U.S.C. § 1349
18 U.S.C. § 1343
18 U.S.C. § 1028A(a)(1)
18 U.S.C. § 2

INDICTMENT

THE GRAND JURY CHARGES:

GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. "The Community" was a loosely organized group of individuals dedicated to online identity theft. A subset of The Community focused on the theft of cryptocurrencies such as Bitcoin, LiteCoin, and Ethereum.

2. Members of The Community planned and organized their activities on various online forums and over diverse channels of communication. Broader discussions—such as discussing the manner and means of attacks generally, and networking among The Community's members—typically took place on forums such as "OGUsers" and "Hackforums." Planning and execution of specific attacks, as well as victim selection and recruiting, usually took place via platforms such as Discord, Skype, Signal, Wickr, and Telegram.

3. The Community engaged in "SIM Hijacking," or "SIM Swapping." This tactic enabled The Community to gain control of a victim's mobile phone number by linking that number to a subscriber identity module ("SIM") card controlled by The Community—resulting in the victim's phone calls and short message service ("SMS") messages being routed to a device controlled by a member of The Community.

4. Once The Community had control of a victim's phone number, it was leveraged as a gateway to gain control of online accounts such as the victim's email, cloud storage, and cryptocurrency exchange accounts. Sometimes this was achieved by requesting a password-reset link be sent via SMS to the device controlled by The Community. Sometimes passwords were compromised by other means, and The Community's device was used to receive two-factor authentication ("2FA") messages sent via SMS intended for the victim.

5. Specific members of The Community endeavored to gain control of a victim's cryptocurrency wallet or online cryptocurrency exchange account and steal the victim's funds. Stolen funds from a successful attack were divided among members of The Community that participated in that attack.

6. During these attacks, one or more members of The Community would appropriate the online identity of the victim, using means of identification including the victim's name, email, and mobile phone number.

7. SIM Hijacking was often facilitated by bribing an employee of a mobile phone provider.

8. Other times, SIM Hijacking was facilitated by "social engineering": a member of The Community would contact a mobile phone provider's customer service—posing as the victim—and request that the victim's phone number be swapped to a SIM card (and thus a mobile device) controlled by The Community.

9. CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), REYAD GAFAR ABBAS (D-4), GARRETT ENDICOTT (D-5), and RYAN STEVENSON (D-6) were members of The Community specializing in the theft of cryptocurrency.

THE SCHEME TO DEFRAUD AND ITS PURPOSE

10. Beginning in approximately December of 2017 and continuing through approximately May of 2018, CONOR FREEMAN (D-1), RICKY

HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), REYAD GAFAR ABBAS (D-4), and GARRETT ENDICOTT (D-5), and RYAN STEVENSON (D-6) defendants herein, in the Eastern District of Michigan and elsewhere did—with the intent to defraud—knowingly participate in a scheme to defraud. The goal of this scheme was to obtain cryptocurrency by means of materially false and fraudulent pretenses and representations.

COUNT ONE

(18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER
D-3 COLTON JURISIC
D-4 REYAD GAFAR ABBAS
D-5 GARRETT ENDICOTT
D-6 RYAN STEVENSON

11. The allegations of paragraphs 1 through 10 are incorporated herein.

12. Beginning in approximately December of 2017 and continuing through approximately May of 2018, in the Eastern District of Michigan and elsewhere, defendants, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), REYAD GAFAR ABBAS (D-4), GARRETT ENDICOTT (D-5), and RYAN STEVENSON (D-6)—along with others known and unknown to the grand jury—did knowingly, intentionally, and willfully combine, conspire, confederate and agree to commit wire fraud. They

knowingly, willfully, and with the intent to defraud—having devised and intending to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, knowing such pretenses, representations, and promises were false and fraudulent when made—transmitted and caused to be transmitted (by means of wire communication) writings, signals, pictures, and sounds in interstate and foreign commerce for the purposes of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

13. The object of the conspiracy was the same as the purpose of the scheme to defraud set forth in paragraph 10 of this Indictment, which is incorporated by reference.

MANNER AND MEANS OF THE CONSPIRACY

14. In furtherance of the conspiracy, and to accomplish its object, the methods, manner, and means that were used are described in paragraphs 1-9 of this Indictment and are incorporated by reference.

All in violation of Title 18, United States Code, Sections 1349

COUNT TWO

(18 U.S.C. §§ 1343 and 2 – Wire Fraud, Aiding and Abetting)

D-4 REYAD GAFAR ABBAS

15. The allegations of paragraphs 1 through 14 are incorporated herein.

16. On or about February 15, 2018, members of The Community collaborated to activate a SIM card and fraudulently link it to the mobile phone number of GP, permitting them to pose as GP.

17. GP's mobile provider was deceived by social engineering into transferring his mobile phone number to a device controlled by The Community.

18. Using GP's mobile phone number as a starting point, one or more members of The Community proceeded to use GP's identity to seize control of multiple online accounts—including an email address, a DropBox account, a cryptocurrency exchange account, and a cryptocurrency wallet.

19. One or more members of The Community transferred cryptocurrency owned by GP, valued at approximately $114,705, to one or more cryptocurrency wallets controlled by The Community.

20. On or about February 15, 2018, REYAD GAFAR ABBAS (D-4) participated in in an online chat furthering the scheme to defraud GP that was transmitted in interstate commerce—including to and from the Eastern District of Michigan.

21. REYAD GAFAR ABBAS (D-4) accessed GP's cryptocurrency exchange account and transferred funds stolen from GP.

22. On or about February 15, 2018, in the Eastern District of Michigan and elsewhere, REYAD GAFAR ABBAS (D-4) and other members of The

Community did—with the intent to defraud—knowingly participate in a scheme to defraud GP by means of false or fraudulent pretenses, representations, or promises.

23. On or about February 15, 2018, in the Eastern District of Michigan and elsewhere, REYAD GAFAR ABBAS (D-4) and other members of The Community used transmission of writings, signs, signals, and sounds sent in interstate commerce in furtherance of the scheme to defraud GP.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT THREE

(18 U.S.C. §§ 1028A(a)(1) and 2 – Aggravated Identity Theft, Aiding and Abetting)

D-4 REYAD GAFAR ABBAS

24. The allegations of paragraphs 1 through 23 are incorporated herein.

25. On or about February 15, 2018, in the Eastern District of Michigan and elsewhere, REYAD GAFAR ABBAS (D-4) and other members of The Community knowingly used identifiers of GP for the purpose of executing the above described scheme to fraudulently obtain cryptocurrency during and in relation to violation of 18 U.S.C. Sections 1343 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT FOUR

(18 U.S.C. §§ 1343 and 2 – Wire Fraud, Aiding and Abetting)

D-5 GARRETT ENDICOTT

26. The allegations of paragraphs 1 through 14 are incorporated herein.

27. On or about March 6, 2018, members of The Community collaborated to activate a SIM card and fraudulently link it to the mobile phone number of TH, permitting them to pose as TH.

28. Using TH's mobile phone number as a starting point, one or more members of The Community proceeded to use TH's identity to seize control of multiple online accounts—including an email account, a Twitter account, cryptocurrency exchange accounts, and a cryptocurrency wallet.

29. One or more members of The Community transferred cryptocurrency owned by TH, valued at approximately $4,929.37, to one or more cryptocurrency wallets controlled by The Community.

30. On or about March 6, 2018, GARRETT ENDICOTT (D-5) participated in an online chat and voice call furthering the scheme to defraud TH that was transmitted in interstate commerce—including to and from the Eastern District of Michigan.

31. GARRETT ENDICOTT (D-5)'s role in The Community was to research victims and to provide personally identifiable information (PII) associated with victims to facilitate the theft of their identities.

32. On or about March 6, 2018, in the Eastern District of Michigan and elsewhere, GARRETT ENDICOTT (D-5) and other members of The Community did—with the intent to defraud—knowingly participate in a scheme to defraud TH by means of false or fraudulent pretenses, representations, or promises.

33. On or about March 6, 2018, in the Eastern District of Michigan and elsewhere, GARRETT ENDICOTT (D-5) and other members of The Community used transmission of writings, signs, signals, and sounds sent in interstate commerce in furtherance of the scheme to defraud TH.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT FIVE

(18 U.S.C. §§ 1028A(a)(1) and 2 – Aggravated Identity Theft, Aiding and Abetting)

D-5 GARRETT ENDICOTT

34. The allegations of paragraphs 1 through 14 and 26 through 33 are incorporated herein.

35. On or about March 6, 2018, in the Eastern District of Michigan and elsewhere, GARRETT ENDICOTT (D-4) and other members of The Community,

knowingly used identifiers of TH for the purpose of executing the above described scheme to fraudulently obtain cryptocurrency during and in relation to violation of 18 U.S.C. Sections 1343 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT SIX

(18 U.S.C. §§ 1343 and 2 – Wire Fraud, Aiding and Abetting)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER
D-3 COLTON JURISIC

36. The allegations of paragraphs 1 through 14 are incorporated herein.

37. On or about May 7, 2018, members of The Community collaborated to activate a SIM card and fraudulently link it to the mobile phone number of JP, permitting them to pose as JP.

38. An employee of a mobile phone provider was bribed by JD, a member of The Community, to transfer the mobile phone number of JP to a SIM card controlled by The Community.

39. In or about May of 2018, JD paid the bribe via LocalBitcoins.com and PayPal, using wire transmissions sent in interstate commerce originating within the Eastern District of Michigan.

40. Using JP's mobile phone number as a starting point, one or more members of the The Community proceeded to use JP's identity to seize control of multiple

online accounts—including an email account, a Twitter account, a cryptocurrency exchange account, and a cryptocurrency wallet.

41. One or more members of The Community transferred cryptocurrency owned by JP, valued at approximately $1,669.56, to one or more cryptocurrency wallets controlled by The Community.

42. On or about May 7, 2018, CONOR FREEMAN (D-1) participated in online chats furthering the scheme to defraud JP that were transmitted in international commerce.

43. CONOR FREEMAN (D-1) provided one or more members of The Community PII of JP that was used to facilitate the attack.

44. On or about May 7, 2018, RICKY HANDSCHUMACHER (D-2) participated in an online chat furthering the scheme to defraud JP that was transmitted in international commerce.

45. RICKY HANDSCHMACHER (D-2) coordinated with JD to further the scheme by prompting JD to bribe an employee of a mobile phone provider to swap the phone number of JP to a device controlled by the Community.

46. The coordination between HANDSHUMACHER and JD was done via an encrypted messaging application that transmitted signals in interstate commerce—including to and from the Eastern District of Michigan—on or about May 7, 2018.

47. On or about May 5, 2018, COLTON JURISIC (D-3) participated in an online chat furthering the scheme to defraud JP that was transmitted in international commerce.

48. COLTON JURISIC (D-3) provided one or more members of The Community with PII of JP that was used to facilitate the attack.

49. In or about May of 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), and other members of The Community did—with the intent to defraud—knowingly participate in a scheme to defraud JP by means of false or fraudulent pretenses, representations, or promises.

50. In or about May of 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), and other members of The Community did use or cause the use of transmission of writings, signs, signals, and sounds sent in international and interstate commerce in furtherance of the scheme to defraud JP.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT SEVEN

(18 U.S.C. §§ 1028A(a)(1) and 2 – Aggravated Identity Theft, Aiding and Abetting)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER
D-3 COLTON JURISIC

51. The allegations of paragraphs 1 through 14 and 36 through 50 are incorporated herein.

52. In or about May of 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), and other members of The Community knowingly used identifiers of JP for the purpose of executing the above described scheme to fraudulently obtain cryptocurrency during and in relation to violation of 18 U.S.C. Sections 1343 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT EIGHT

(18 U.S.C. §§ 1343 and 2 – Wire Fraud, Aiding and Abetting)

D-4 REYAD GAFAR ABBAS

53. The allegations of paragraphs 1 through 14 are incorporated herein.

54. On or about May 9, 2018, members of The Community collaborated to activate a SIM card and fraudulently link it to the mobile phone number of AL, permitting them to pose as AL.

55. An employee of a mobile phone provider was bribed by JD, a member of The Community, to transfer the mobile phone number of AL to a SIM card controlled by The Community.

56. In or about May of 2018, JD paid the bribe via LocalBitcoins.com and PayPal, using wire transmissions sent in interstate commerce originating within the Eastern District of Michigan.

57. Using AL's mobile phone number as a starting point, one or more members of The Community proceeded to use AL's identity to seize control of multiple online accounts—including an email account, a Skype account, and a cryptocurrency exchange account.

58. One or more members of The Community transferred cryptocurrency owned by AL, valued at approximately $55,493.76, to one or more cryptocurrency wallets controlled by The Community.

59. On or about dates between May 9, 2018 and May 13, 2018, REYAD GAFAR ABBAS (D-4) participated in online chats furthering the scheme to defraud AL that were transmitted in interstate commerce—including to and from the Eastern District of Michigan.

60. REYAD GAFAR ABBAS (D-4) accessed AL's email account to facilitate the attack and transferred funds stolen from AL.

61. In or about May of 2018, in the Eastern District of Michigan and elsewhere, REYAD GAFAR ABBAS (D-4) and other members of The Community did—with the intent to defraud—knowingly participate in a scheme to defraud AL by means of false or fraudulent pretenses, representations, or promises.

62. In or about May of 2018, in the Eastern District of Michigan and elsewhere, REYAD GAFAR ABBAS (D-4) and other members of The Community used or caused the use of transmission of writings, signs, signals, and sounds sent in interstate commerce in furtherance of the scheme to defraud AL.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT NINE

(18 U.S.C. §§ 1028A(a)(1) and 2 – Aggravated Identity Theft, Aiding and Abetting)

D-4 REYAD GAFAR ABBAS

63. The allegations of paragraphs 1 through 14 and 53 through 62 are incorporated herein.

64. In or about May of 2018, in the Eastern District of Michigan and elsewhere, REYAD GAFAR ABBAS (D-4) and other members of The Community knowingly used identifiers of AL for the purpose of executing the above

described scheme to fraudulently obtain cryptocurrency during and in relation to violation of 18 U.S.C. Section 1343 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT TEN

(18 U.S.C. §§ 1343 and 2 – Wire Fraud, Aiding and Abetting)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER
D-3 COLTON JURISIC

65. The allegations of paragraphs 1 through 14 are incorporated herein.

66. On or about May 15, 2018, members of The Community collaborated to activate a SIM card and fraudulently link it to the mobile phone number of DM, permitting them to pose as DM.

67. An employee of a mobile phone provider was bribed by JD, a member of The Community, to provide PII of DM that enabled a member of The Community to impersonate DM and convince a customer service representative to transfer the mobile phone number of DM to a SIM card controlled by The Community.

68. In or about May of 2018, JD paid the bribe via LocalBitcoins.com and PayPal, using wire transmissions sent in interstate commerce originating within the Eastern District of Michigan.

69. Using DM's mobile phone number as a starting point, members of The Community proceeded to use DM's identity to seize control of multiple online

accounts—including an email account, cloud storage accounts, and a cryptocurrency wallet.

70. One or more members of The Community transferred cryptocurrency owned by DM, valued at approximately $100,000, to cryptocurrency wallets controlled by members of The Community, including CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2) and COLTON JURISIC (D-3).

71. On or about May 15, 2018, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), and COLTON JURISIC (D-3) participated in an online chat furthering the scheme to defraud DM that was transmitted in international and interstate commerce—including to and from the Eastern District of Michigan.

72. CONOR FREEMAN (D-1) provided one or more members of The Community with PII of DM that was used to facilitate the attack.

73. CONOR FREEMAN (D-1) transferred funds stolen from DM.

74. COLTON JURISIC (D-3), provided one or more members of The Community with PII of DM that was used to facilitate the attack.

75. On or about May 15, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), and other members of The Community did—with the intent to

defraud—knowingly participate in a scheme to defraud DM by means of false or fraudulent pretenses, representations, or promises.

76. On or about May 15, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3) and other members of The Community did use or cause the use of transmission of writings, signs, signals, and sounds sent in international and interstate commerce in furtherance of the scheme to defraud DM.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT ELEVEN

(18 U.S.C. §§ 1028A(a)(1) and 2 – Aggravated Identity Theft, Aiding and Abetting)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER
D-3 COLTON JURISIC

77. The allegations of paragraphs 1 through 14 and 65 through 76 are incorporated herein.

78. On or about May 15, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), COLTON JURISIC (D-3), and other members of The Community knowingly used identifiers of DM for the purpose of executing the above described scheme to

fraudulently obtain cryptocurrency during and in relation to violation of 18 U.S.C. Section 1343 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT TWELVE

(18 U.S.C. §§ 1343 and 2 – Wire Fraud, Aiding and Abetting)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER

79. The allegations of paragraphs 1 through 14 are incorporated herein.

80. On or about May 16, 2018, members of The Community collaborated to activate a SIM card and fraudulently link it to the mobile phone number of SS, permitting them to pose as SS.

81. An employee of a mobile phone provider was bribed by JD, a member of The Community, to facilitate the transfer of the mobile phone number of SS to a SIM card controlled by The Community.

82. In or about May of 2018, JD paid the bribe via LocalBitcoins.com and PayPal, using wire transmissions sent in interstate commerce originating within the Eastern District of Michigan.

83. Using SS's mobile phone number as a starting point, members of The Community proceeded to use SS's identity to seize control of multiple online

accounts—including an email account, an Evernote account, cryptocurrency exchange accounts, and cryptocurrency wallets.

84. One or more members of The Community transferred cryptocurrency controlled and possessed by SS, valued at approximately $1,921,335.80, to one or more cryptocurrency wallets controlled by The Community.

85. On or about May 16, 2018, CONOR FREEMAN (D-1) and RICKY HANDSCHUMACHER (D-2) participated in an online chat furthering the scheme to defraud SS that was transmitted in international and interstate commerce—including to and from the Eastern District of Michigan.

86. CONOR FREEMAN (D-1) transferred funds that were stolen from SS.

87. On or about May 16, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), and other members of The Community did—with the intent to defraud—knowingly participate in a scheme to defraud SS by means of false or fraudulent pretenses, representations, or promises.

88. On or about May 16, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), and other members of The Community did use or cause the use of transmission of writings, signs, signals, and sounds sent in international and interstate commerce in furtherance of the scheme to defraud SS.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT THIRTEEN

(18 U.S.C. §§ 1028A(a)(1) and 2 – Aggravated Identity Theft, Aiding and Abetting)

D-1 CONOR FREEMAN
D-2 RICKY HANDSCHUMACHER

89. The allegations of paragraphs 1 through 14 and 79 through 88 are incorporated herein.

90. On or about May 16, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), RICKY HANDSCHUMACHER (D-2), and other members of The Community knowingly used identifiers of SS for the purpose of executing the above described scheme to fraudulently obtain cryptocurrency during and in relation to violation of 18 U.S.C. Section 1343 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT FOURTEEN

(18 U.S.C. §§ 1343 and 2 – Wire Fraud, Aiding and Abetting)

D-1 CONOR FREEMAN
D-3 COLTON JURISIC

91. The allegations of paragraphs 1 through 14 are incorporated herein.

92. On or about May 18, 2018, members of The Community collaborated to activate a SIM card and fraudulently link it to the mobile phone number of MT, permitting them to pose as MT.

93. An employee of a mobile phone provider was bribed by JD, a member of The Community, to transfer the mobile phone number of MT to a SIM card controlled by The Community.

94. In or about May of 2018, JD paid the bribe via LocalBitcoins.com and PayPal, using wire transmissions sent in interstate commerce originating within the Eastern District of Michigan.

95. Using MT's mobile phone number as a starting point, one or more members of The Community proceeded to use MT's identity to seize control of multiple online accounts—including email and cryptocurrency exchange accounts.

96. One or more members of The Community transferred cryptocurrency owned by MT, valued at approximately $164,972.47, to one or more cryptocurrency wallets controlled by The Community.

97. On or about May 18, 2018, CONOR FREEMAN (D-1) and COLTON JURISIC (D-3) participated in an online chat furthering the scheme to defraud MT that was transmitted in international and interstate commerce—including to and from the Eastern District of Michigan.

98. CONOR FREEMAN (D-1) accessed MT's email and cryptocurrency exchange accounts, and transferred funds stolen from MT.

99. COLTON JURISIC (D-3) provided one or more members of The Community with PII of MT that was used to facilitate the attack.

100. On or about May 18, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), COLTON JURISIC (D-3), and other members of The Community did—with the intent to defraud—knowingly participate in a scheme to defraud MT by means of false or fraudulent pretenses, representations, or promises.

101. On or about May 18, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), COLTON JURISIC (D-3), other members of The Community did use or cause the use of transmission of writings, signs, signals, and sounds sent in international and interstate commerce in furtherance of the scheme to defraud MT.

All in violation of Title 18, United States Code, Section 1343 and 2.

COUNT FIFTEEN

(18 U.S.C. §§ 1028A(a)(1) and 2 – Aggravated Identity Theft, Aiding and Abetting)

D-1 CONOR FREEMAN
D-3 COLTON JURISIC

102. The allegations of paragraphs 1 through 14 and 91 through 101 are incorporated herein.

103. On or about May 17, 2018, in the Eastern District of Michigan and elsewhere, CONOR FREEMAN (D-1), COLTON JURISIC (D-3), and other members of The Community knowingly used identifiers of MT for the purpose of executing the above described scheme to fraudulently obtain cryptocurrency during and in relation to violation of 18 U.S.C. Section 1343 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATIONS

104. Upon conviction of Wire Fraud, in violation of Title 18, United States Code, Section 1343, as alleged in Counts 2, 4, 6, 8, 10, 12, and 14, of this Indictment, and Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349, defendants shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) together with 28 U.S.C. § 2461(c), their right, title and interest in any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses.

105. Upon conviction of Aggravated Identity Theft, in violation of Title 18, United States Code, Sections 1028(a)(1), as alleged in Counts 3, 5, 7, 9, 11, 13, and 15, of this Indictment, defendants shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1028(b), their right, title, and interest in: (i) any

property constituting, or derived from, proceeds the person obtained directly or indirectly, as a result of the offense(s), and (ii) any personal property used or intended to be used to commit the offense(s).

106. Forfeiture Money Judgment: Upon conviction of Wire Fraud, in violation of Title 18, United States Code, Section 1343, as alleged in Counts 1, 3, 5, 7, 9, 11, and 13, of this Indictment, and/or Aggravated Identity Theft, a violation of Title 18, United States Code, Section 1028(a)(1), as alleged in Counts 2, 4, 6, 8, 10, 12, and 14, of this Indictment, defendants shall be ordered to pay a sum of money equal to the amount of proceeds obtained as a result of their offense(s).

107. Substitute Assets: Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), Defendants shall forfeit substitute property, up to the value of the property subject to forfeiture as set forth above, if, by any act or omission of the defendant, property subject to forfeiture cannot be located upon the exercise of due diligence; has been transferred, sold to or deposited with a third party; has been placed beyond the jurisdiction of the court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.

THIS IS A TRUE BILL

/s/ Grand Jury Foreperson
GRAND JURY FOREPERSON

MATTHEW SCHNEIDER
UNITED STATES ATTORNEY

/s/ John K. Neal
John K. Neal
Assistant United States Attorney
Chief, White Collar Crime Unit

/s/ Timothy J. Wyse
Timothy J. Wyse
Assistant United States Attorney
211 West Fort Street, Suite 2001
Detroit, MI 48226
Timothy.Wyse@usdoj.gov
(313) 226-9144

Dated: April 18, 2018

ORIGINAL

United States District Court Eastern District of Michigan	**Criminal Case**	Case:2:19-cr-20246 Judge: Hood, Denise Page MJ: Patti, Anthony P. Filed: 04-18-2019 At 04:44 PM SEALED MATTER (dat)

NOTE: It is the responsibility of the Assistant U.S. Attorney signing this form t

Companion Case Information	**Companion Case Number:**
This may be a companion case based upon **LCrR 57.10 (b)(4)**[1]:	**Judge Assigned:**
☐ **Yes** ☒ **No**	**AUSA's Initials:** TJW

Case Title: USA v. D-1 Conor Freeman, et al.

County where offense occurred : Wayne

Check One: ✓ ☒**Felony** ☐**Misdemeanor** ☐**Petty**

____Indictment/__✓__Information --- **no** prior complaint.
____Indictment/____Information --- based upon prior complaint [**Case number:**]
____Indictment/____Information --- based upon **LCrR 57.10 (d)** ***[Complete Superseding section below]***.

Superseding Case Information

Superseding to Case No: _____ **Judge:** _____

☐Corrects errors; no additional charges or defendants.
☐Involves, for plea purposes, different charges or adds counts.
☐Embraces same subject matter but adds the additional defendants or charges below:

Defendant name	**Charges**	**Prior Complaint (if applicable)**

Please take notice that the below listed Assistant United States Attorney is the attorney of record for the above captioned case.

April 18, 2019
Date

Timothy J. Wyse
Assistant United States Attorney
211 W. Fort Street, Suite 2001
Detroit, MI 48226-3277
Phone: (313) 226-9144
Fax: (313) 226-2873
E-Mail address: Timothy.Wyse@usdoj.gov
Attorney Bar #:

[1] Companion cases are matters in which it appears that (1) substantially similar evidence will be offered at trial, or (2) the same or related parties are present, and the cases arise out of the same transaction or occurrence. Cases may be companion cases even though one of them may have already been terminated.

EXHIBIT B

Regional Enforcement Allied Computer Team **INVESTIGATION REPORT:** **COVER AND PARTY PAGES**	Case Number: 2018-0066		
	Occurred	Date	Time
	ON OR FROM	Oct 15, 2018	12:00:00 AM
Report Type: 502(c)(1) PC Unlawful Computer Access, 487(a) PC Grand Theft, 530.5(a) PC ID Th	TO	Oct 26, 2018	12:00:00 AM
Location of Crime: 605 West 42nd Street 64W, New York, New York 10036	REPORTED	Oct 19, 2018	12:00:00 AM

SUSPECT INFORMATION AND ASSOCIATED CHARGES

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
1	Truglia, Nicholas	[redacted]	21	M	White	6'3"	200

Home Address	City	State	Zip Code
[redacted]	New York	NY	10036

Phone Number/Type	E-mail Address	DL #	PFN	CII #	Social Security #
[redacted]		[redacted]			[redacted]

Applicable Charge	Description of Charge	
502(c)(1) PC	Unlawful Computer Access	
487(a) PC	Grand Theft	
530.5(a) PC	Identity Theft	
664/487(a) PC	Attempted Grand Theft	

INVOLVED PARTY INFORMATION

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
1	Basu, Saswata	[redacted]	48	M	A		

Address	City	State	Zip Code
[redacted]	Cupertino	CA	95014

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]			Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
2	Ross, Robert	[redacted]	55	M	White		

Address	City	State	Zip Code
[redacted]	San Francisco	CA	94118

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
3	Anderson, Angel	[redacted]	46	F	W		

Address	City	State	Zip Code
[redacted]	Los Angeles	CA	90046

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]			[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
4	Danielson, Myles Walker	[redacted]	33	M	W		

Address	City	State	Zip Code
[redacted]	San Francisco	CA	94109

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
5	Katsnelson, Gabrielle	[redacted]	34	F	W		

Address	City	State	Zip Code
[redacted]	San Francisco	CA	94133

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

SYNOPSIS:

Victim Saswata Basu, a resident of Santa Clara County, had his AT&T cell phone taken over by the suspect who then gained unlawful access to V. Basu's Yahoo email account and attempted to access his Dropbox account. I was also contacted by Victim Ross who lost access to his cell phone, Gmail account and had approximately $1,000,000 stolen from two cryptocurrency exchanges where the suspects transferred USD into Bitcoin and transferred funds into cryptocurrency wallets the suspects controlled. The suspect also attempted to wire transfer approximately $300,000 from Victim Danielson's Fidelity account but was stopped by the victim. The victims listed in this investigation live within the greater San Francisco Bay Area and Southern California.

BACKGROUND DEFENITIONS:

"Cryptocurrency": Any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

"SIM card": For some types of mobile communication devices, a Subscriber Identity Module (or "SIM") card is a small card that is inserted into a mobile device (such as a cell phone handset) to enable the mobile device to communicate with its service provider, as it contains network data needed to make a successful connection to the cellular network provider. SIM cards store files that can be used to uniquely identify them, including the ICCID (Integrated Circuit Card Identifier, a 19- or 20-digit serial number for the SIM card that uniquely identifies the card itself) and the IMSI (International Mobile Subscriber Identity, a 14-or 15- digit number that uniquely identifies a subscriber's account with the cellular network provider).

"SIM swap": An account takeover method by which cellular phone service accounts are compromised. In this scheme, the suspect arranges (through bribery of someone with access,

artifice/"social engineering," or other methods) for a cellular service provider to change the SIM card assigned to particular account to a new SIM card under the suspect's control. Once the suspect controls the new SIM card, he/she can impersonate the victim in correspondence with other service providers (such as email providers) by using the victim's cell phone number to request changes to account settings, eventually resetting the password and taking control of the account.

"IMEI": IMEI is short for International Mobile Equipment Identity is a 15 or 17 digit number that is used to uniquely identify certain types of mobile phone devices. Many providers of electronic communication services log the IMEI number used to access their systems.

2-Factor Authentication ("2FA"): A security mechanism that requires two types of credentials for authentication and is designed to provide an additional layer of validation.

INVESTIGATION:

(V) Saswata B.

Saswata B. is a resident of Santa Clara County. He is a previously reported victim of a SIM swap that occurred in May of 2018 that has been investigated by the REACT Task Force. On 10/18/18, he notified Santa Clara Sheriff's Office Sergeant S. Tarazi that he had just been the victim of another SIM swap, where the target was his phone number ending in -3543. During the incident, the suspects unlawfully accessed his Yahoo email but did not steal any currency or cryptocurrency. AT&T provided records which indicated the mobile communication device utilizing the SIM card used to take over the victim's account during this SIM swap was assigned the IMEI 359239069326461.

(V) Robert R.

On 10/27/1818, at approximately 0800 hours, I began receiving text messages (depicted below) on my department issued cell phone from a phone number [redacted] which I did not recognize.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

I called the number and the voice of a panicked male adult identified himself as (V) Robert R. He gave me the following paraphrased statement over the phone and through email communications:

Robert R. is a resident of San Francisco, California. On 10/26/18, at approximately1800 hours, his cell phone, which uses a phone number ending in -6433, started getting notifications from the "Authy" application seen below which the suspect was controlling.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Gemini is a cryptocurrency exchange in which Robert R. had approximately $500,000 USD, and he had approximately $500,000 more was in a similar account with cryptocurrency exchange Coinbase. At approximately the same time he saw the messages above, Robert R. lost cell service, was logged out of and lost access to his Gmail account ([redacted]), and the suspects took over his "Authy" 2-factor authentication application. He realized a theft was in progress as he could not access any accounts (Gmail, Authy, AT&T or cryptocurrency accounts). He immediately went to an Apple Store where representatives helped him call AT&T Customer Support, who told the victim his SIM card had been changed. Apple inserted a new SIM into his cell phone and AT&T activated the new SIM card, which restored his access to his own phone service.

When this occurred, all of Robert R.'s funds stored on Coinbase (approximately $500,000) and Gemini (approximately $500,000) had been held in USD. The suspect used all the funds in USD at both exchanges to purchase bitcoins, then immediately withdrew all of the bitcoins. Robert R. found this out by looking at transactions on his CoinTracking account, which is connected to his Coinbase and Gemini exchange accounts. This information was subsequently verified by obtaining records directly from Coinbase and Gemini via search warrant.

Robert R. told me he did not sleep at all that night and was up trying to get access to his accounts, figuring out how to retrieve his stolen money and finding someone to help him with the theft. Although he had access to his phone, he was still locked out of his Gmail account, Authy security application, and all of his cryptocurrency accounts. The money stolen was his life savings and money earmarked for his daughter's college fund. He told me many times that he was not sure how he was going to live the rest of his life and send his daughter to college without this money.

Search Warrant to AT&T for records pertaining to IMEI 359239069326461

On 10/29/18, the Honorable Linda Clark, Judge of the Superior Court, signed a search warrant for AT&T records pertaining to accounts linked to the IMEI number 359239069326461. In response, AT&T provided REACT investigators with records that showed the mobile device bearing that IMEI number had been used to effect the account takeovers of both of the victims described above, Saswata B. and Robert R., as well as those of other victims. In total, the records indicated that 11 unique phone numbers had been SIM swapped using this device between 10/15/18 and 10/26/18.

I spoke with the following additional victims who were among the victims listed and whose accounts were taken over using the device bearing IMEI 359239069326461:

(V) Myles D.

I met with this victim in person on 11/6/18 at approximately 0800 hours, and he related the following. Myles D. lives in San Francisco, California. On 10/26/18, at approximately 1530 hours, Myles D.'s

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

AT&T cell phone ([redacted] stopped working while he was at an appointment. Approximately an hour later he confirmed with his wife that her phone was also not working. At approximately 1700 hours, he went to an AT&T Store to try and resolve the issue. The AT&T Store employee pulled the SIM card from his phone and compared the SIM card to the SIM card listed in the account and realized the numbers were different. The employee changed the SIM card back to the original SIM card number and Myles D. regained access to his cell phone service. Once he had phone service back, he checked his Gmail account ([redacted] and learned it was disabled by Google. He contacted Google and had his email access restored, and found out that the suspects had accessed his Gmail account for approximately 4 minutes before Google realized the access was unauthorized and Google disabled the account.

At approximately 1800 hours, he returned to his workplace to look into the hack further because he felt using work computers was safer. He looked in his Gmail account and saw an email from an unknown subject with a Gmail address stating this person knew who had hacked him and seemed to be offering assistance. He forwarded that email to Google to see if Google could tell him anything about that account. A short time later he received a telephone call from a blocked number. The voice on the other line stated they were in a "Dark Web" chat room and a group of subjects were talking about going after the victim's cryptocurrency accounts. Myles D. does not have any cryptocurrency but works for a company which is involved in cryptocurrency. He was scared and believed he was talking to the hackers, and hung up the phone.

On 10/28/18, Myles D. received an email from Fidelity informing him that three of his mutual fund accounts had been liquidated and were pending wire transfers. He contacted Fidelity and was able to cancel the wire transfers. The suspect(s) had attempted to transfer approximately $300,000 from the victim's Fidelity account.

(V) Angel A.

I spoke with this victim via telephone on 11/1/18, and she related the following. Angel A. is a resident of Los Angeles, California. On 10/16/18, her AT&T cell phone number ([redacted] stopped

working. A short time later she realized she had lost access to her Twitter social media account ([redacted]). The suspect who was in control of [redacted] began sending bomb threats to airlines from her Twitter account along with racist "Tweets" regarding Former President Barack Obama. The victim contacted Twitter and regained access to her account. She is unaware of any other accounts that were compromised.

(V) James M.

I spoke with this victim via telephone on 11/1/18, and he related the following. James M. is a resident of Bronx, New York. On 10/15/18, his AT&T cell phone number ([redacted]) stopped working. He received an email from Instagram that the password was changed for his Instagram username ([redacted] and the email account associated to his [redacted] Instagram account was changed to [redacted]. The suspect attempted to access his Facebook account, but Facebook stopped the attempt. He believes somebody with the Instagram account @gay hacked him because the victim was taunted on his new Instagram Account by that user via Instagram Direct Message for having lost access to [redacted]. The victim was never able to regain access to [redacted], which he had used for business purposes.

(V) Gabrielle K.

I spoke with this victim via telephone on 10/30/18, and she related the following. Gabrielle K. is a resident of San Francisco. On 10/21/18, her AT&T cell phone number ([redacted]) stopped working. She noticed this when she woke up and her had phone no service. She received an email from AOL that her password was changed and a Gmail notification that her Gmail, Evernote and Dropbox passwords had changed. She also received a notice that her Coinbase cryptocurrency account login information had changed. She was able to disable her Coinbase account before any further actions were taken by the suspect. She then went to an AT&T Store to get a new SIM card.

(V) Matthew R.

I spoke with this victim via telephone on 11/2/18, and he related the following. Matthew R. is a resident of the State of Texas. On 10/23/18, his AT&T cell phone number ([redacted]) stopped

working. While he was still connected on Wi-Fi, he received emails that his email account passwords were reset. He was still logged into those accounts while the suspect was simultaneously in control. He saw emails saying other accounts connected to the email were being reset. Those accounts included [redacted] and [redacted] The suspect also attempted to gain access to his Coinbase, HitBTC, Binance and Bittrex cryptocurrency accounts and his blockchain cryptocurrency wallet. The suspects called him twice asking for blackmail payments of $200,000 in Bitcoin to get all his accounts back. One of the suspects sounded young and Asian and the second suspect sounded Eastern European and seemed like he was trying to disguise his voice.

Suspect telephone number [redacted] and identification of (S) Nicholas TRUGLIA

Records provided by AT&T also indicated that the when the suspect's phone was in control of the identified victim accounts, the phone was located in the New York, New York area. In addition, the records indicated that the phone number [redacted] was connected to the suspect IMEI (359239069326461) on 10/5/18, but that this connection was not reported as a fraudulent SIM Swap by the customer. I believe this is indicative of the suspect using a SIM card in his/her possession to test whether the cell phone is functioning properly and connects to the cell carrier's network. I therefore believe the phone number [redacted] belonged to the suspect.

On 10/26/18, the Honorable Maureen Folan, Judge of the Superior Court, signed a search warrant for AT&T records pertaining to the account associated with the telephone number [redacted]. AT&T provided REACT investigators with records that identified the subscriber as "Jeffrey St. Denis" and included the additional information described below.

On 10/29/18, the cryptocurrency exchange Coinbase provided records to investigators which identified an account associated with the phone number [redacted] the number believed to be associated with the suspect. These records indicated this phone number was used to register a Coinbase account in the name of Nicholas TRUGLIA using the social security number [redacted] and the email

address [redacted]. Another name associated with the account was Jeffrey St. Denis, the same name as shown in AT&T subscriber records for the suspect phone number. The records also included copies of documents the subscriber used to identify himself, which included a Connecticut Driver License in the name of Nicholas TRUGLIA with a date of birth of [redacted] and a U.S. passport in the name of Nicholas St. Denis TRUGLIA (note the middle name that matches the name used in AT&T subscriber information from the suspect account) with a date of birth of [redacted]

TRUGLIA's Coinbase account also showed deposits and withdrawals of cryptocurrency occurring between 1/6/16 and 3/24/18, and then no activity after 3/24/18 until 10/27/18. On 10/27/18, mere hours after the theft of the bitcoins described above, as well as approximately 14.3 Ether ("ETH") from (V) Robert R.'s account with the cryptocurrency exchange Binance, a small amount of Ether (approximately .025 ETH) was deposited into TRUGLIA's Coinbase account. Santa Clara County District Attorney Investigator D. Berry received records pertaining to Robert R.'s account from Binance on 10/27/18 that reflected the 14.3 ETH theft from Robert R.'s account, although that stolen ETH was transferred only once to an exterior address, and has not moved from that address as of the writing of this report.

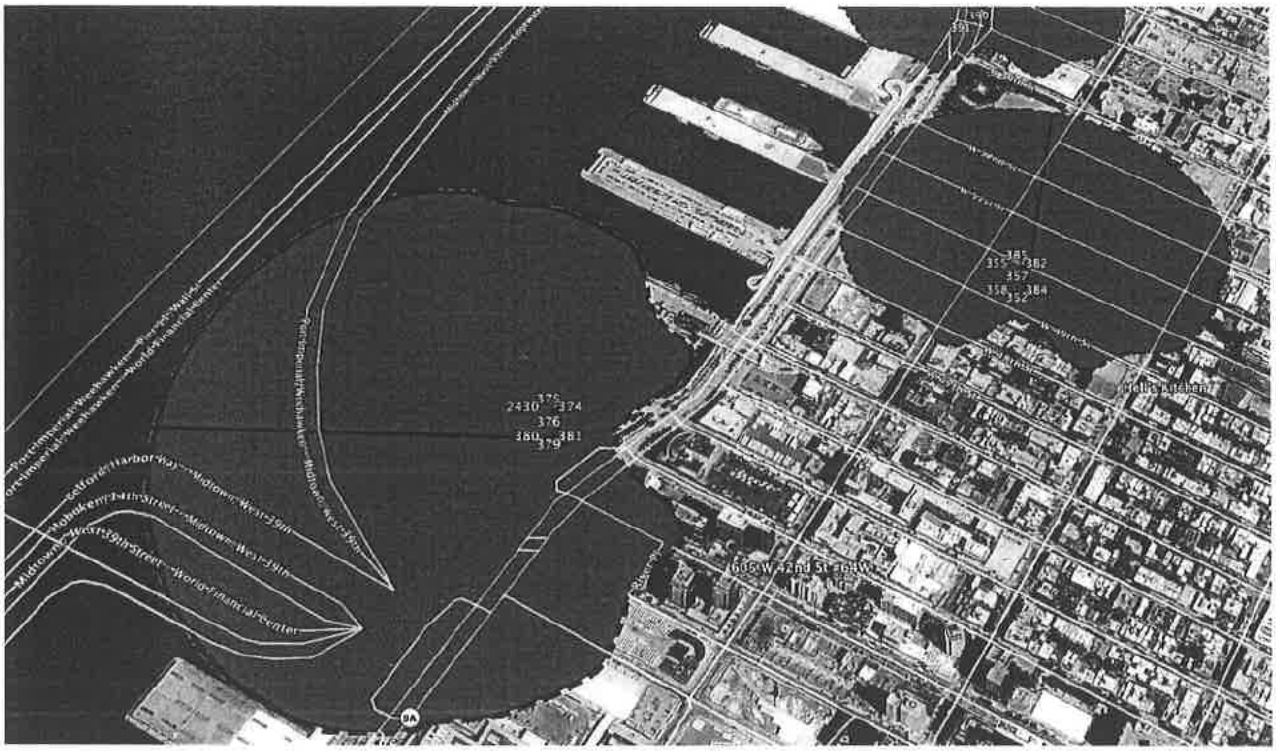
On 11/6/18, REACT investigators received records from the State of New York showing Nicholas TRUGLIA had a New York State Identification Card which listed an address of [redacted], New York 10036.

Sgt. Tarazi examined the records obtained from AT&T and arrived at the following conclusions, in summary (see Sgt. Tarazi's supplemental report for details):

- The records pertaining to TRUGLIA's cell phone account ([redacted]) indicate the owner of the AT&T phone number [redacted] was assigned a SIM card that was physically inserted into an iPhone X with IMEI ending in -5311. Someone removed the SIM card form this iPhone X and placed it inside an iPhone 6 with IMEI ending in -6461, which is the device used to effect the SIM swaps. After approximately 18 minutes, someone removed the SIM

card from the iPhone 6 (-6461) and put it back into the iPhone X (-5311). This SIM card has remained inside the iPhone X (5311) since it was put back in.

- The AT&T cell phone towers to which the iPhone 6 (6461) was connected during the approximate 2 hours and 10 minutes it was in control of victim Matthew R.'s account was consistent with the device having been located at [redacted] NY, as depicted below:



- During that same time period, that same AT&T cell phone tower, as well as several other nearby towers, were used by the iPhone X associated with TRUGLIA's account (5211), as depicted below.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Prior Attempted Account Takeover involving TRUGLIA

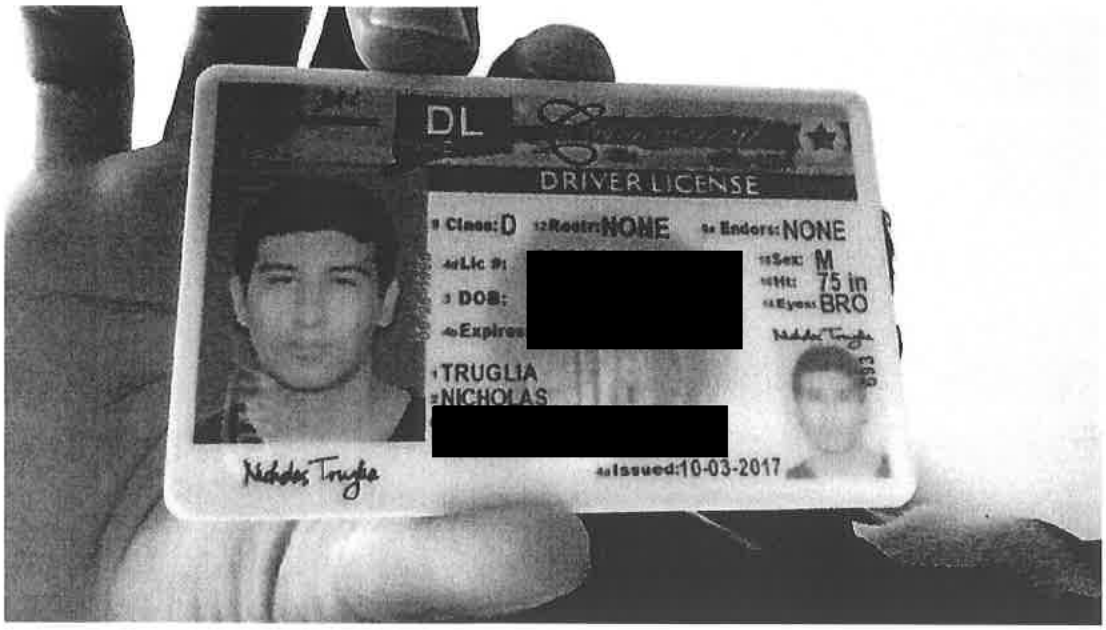
On 10/31/18, Coinbase provided additional information indicating that Truglia has previously been involved in account takeover activity. Coinbase informed REACT investigators that in mid-May 2018, Coinbase received an anonymous tip that someone was going to hack into the Coinbase account of Quinten Capobianco, who had previously died. After Coinbase secured the target account, an external attempt was made to access the account. Coinbase prompted the suspect to provide a photograph of himself holding his ID card as verification, and in response the suspect provided the photograph below.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Based on a comparison to known images, I recognize the person in the photograph above as Nicholas Truglia, who is holding what appears to be a false New York State driver license in Capobianco's name but bearing Truglia's image. Furthermore, Coinbase records indicated that the same device that attempted to access Capobianco's account was then used to log into Truglia's account.

The following three photos were provided as proof of identity for the other Coinbase accounts opened in Truglia's name:

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE



Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The following picture is from Truglia's New York Identification, which was obtained through a law enforcement database.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

DMV Photo Request

DMV Photo

Subject Information	
Name:	TRUGLIA,NICHOLAS,S
ClientID:	161405797
Case Number:	108711
DMV Transaction Number:	756281
DMV Transaction Date/Time:	2018-11-05 15:38:31:767

Back

I believe all of the pictures above depict Truglia.

Based on this information, I believe Suspect Truglia attempted to access the deceased person's Coinbase account. This behavior is consistent with the SIM Swapping activity described in this report in the use of impersonation techniques to steal cryptocurrency.

Laundering of stolen funds

Santa Clara County District Attorney Criminal Investigator D. Berry, a REACT Task Force investigator, has examined the flows of cryptocurrency out of Robert R.'s Coinbase, Gemini, and Binance accounts. Investigator Berry observed that the bitcoins transferred out of his Coinbase and Gemini accounts were initially aggregated into a single Bitcoin address, and then moved in a series of transactions that appear intended to obfuscate the source and destination of funds. After some of those layers of movement, proceeds of the theft were deposited into accounts at Binance, a cryptocurrency exchange based in Malta, in a series of transactions apparently structured to avoid account registration requirements (just under 2 bitcoins per transaction, which is the limit above which an account involving "customer due diligence" must be established). Binance provided information related to those transactions, which showed that a series of accounts exhibiting similar behavior had received,

and then promptly withdrawn, the identified stolen bitcoins, which were then aggregated into some overlapping Bitcoin addresses. *See Investigator Berry's supplemental report for additional details.*

Based on my training and experience, I know that moving stolen cryptocurrency through multiple addresses, breaking up stolen amounts into multiple segments of smaller amounts, structuring flows to avoid reporting requirements, and taking steps to avoid meaningful customer due diligence are all consistent with money laundering efforts.

CONCLUSION

Based on the statements of the victims, IMEI number 359239069326461 being connected to S-TRUGLIA's personal cell phone line, Sgt. Tarazi's analysis of phone records, and Investigator Berry's analysis regarding cryptocurrency tracing, I believe S-TRUGLIA committed the following crimes detailed below:

V-Ross:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account

487(a) PC – Theft of approximately $500,000 from his Coinbase account

487(a) PC – Theft of approximately $500,000 from his Gemini account

V-Anderson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Twitter account and sending messages

V-Danielson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account

502(c)(1) PC and 664/487(a) PC – Unlawfully Accessing Fidelity Mutual Fund and attempting to wire $300,000 from the account

V-Katsnelson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Dropbox account

502(c)(1) PC – Unlawfully Accessing Evernote account

502(c)(1) PC – Unlawfully Accessing Coinbase account

V-Basu:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Yahoo account

664/502(c)(1) PC– Unlawfully Attempting to Access Dropbox account

I am requesting the Santa Clara County District Attorney's Office issue a warrant for the arrest of S-TRUGLIA for the above listed charges.

END REPORT.

PLEO:

TFA C. Tuttle #1945 – Original report
TFA S. Tarazi #2029 – Cell Tower/Geolocation Supplemental Report
TFA D. Berry #47 -- Cryptocurrency Tracing Supplemental Report

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Supplemental Report

Investigation:

On 10-27-2018, REACT detectives received a spreadsheet file from AT&T Fraud Investigator Robert Arno entitled "359239069326461 updated 102718." The first number represents an IMEI number that had been used to conduct SIM swaps. These phone numbers had been identified by AT&T as being used on the above listed IMEI, belonging to an iPhone 6. This IMEI will be referred to by the last 4 digits (6461) throughout the report.

Mobile Number	SIM Card Number	First Use Date
[redacted]	310410704975735	Fri Oct 26 19:50:27 EDT 2018
	310410704975631	Fri Oct 26 17:41:20 EDT 2018
	310410704975737	Wed Oct 24 20:37:24 EDT 2018
	310410704975708	Tue Oct 23 19:44:54 EDT 2018
	310410916138275	Mon Oct 22 23:48:25 EDT 2018
	310410704975736	Sun Oct 21 12:50:23 EDT 2018
	310410704975738	Thu Oct 18 15:37:36 EDT 2018
	310410704975632	Tue Oct 16 14:35:07 EDT 2018
	310410704975633	Mon Oct 15 19:30:26 EDT 2018
	310410704975629	Mon Oct 15 18:31:02 EDT 2018
	310410704975630	Mon Oct 15 15:22:49 EDT 2018
	310410074713285	Fri Oct 05 19:24:43 EDT 2018

Each number above, except for [redacted], was identified by Robert Arno as being an account victimized by an unauthorized SIM Swap by the IMEI ending is 6461. Several of the numbers above have been identified as victims of cryptocurrency theft. See Detective Tuttle's Supplemental Report for further details.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The number [redacted] has been identified as belonging to Suspect Truglia. The phone number had been used to register for a PayPal and Coinbase account in Suspect Truglia's name. See Detective Berry's Supplemental report for further details.

I authored and served a Search Warrant for AT&T records regarding IMEI number ending in 6461 (iPhone 6). I received partial record returns which included the call detail records for the phone number [redacted] and the subscriber information for the rest of the numbers listed above.

Detective Tuttle authored and served a Search Warrant for AT&T records regarding the phone number [redacted] (Suspect Truglia's AT&T phone number).

I examined the call detail records for Suspect Truglia's phone line and I noticed that on 10-5-18 at 23:24:43 (UTC) the IMEI number on the account switched from 354851092905311 (iPhone X) to the iPhone 6 ending in 6461. The records indicate the IMEI switched back to the iPhone 10 (5311) at 23:43:54 (UTC), approximately 18 minutes later. The iPhone X (5311) has been assigned to the Suspect Truglia's account since it switched back.

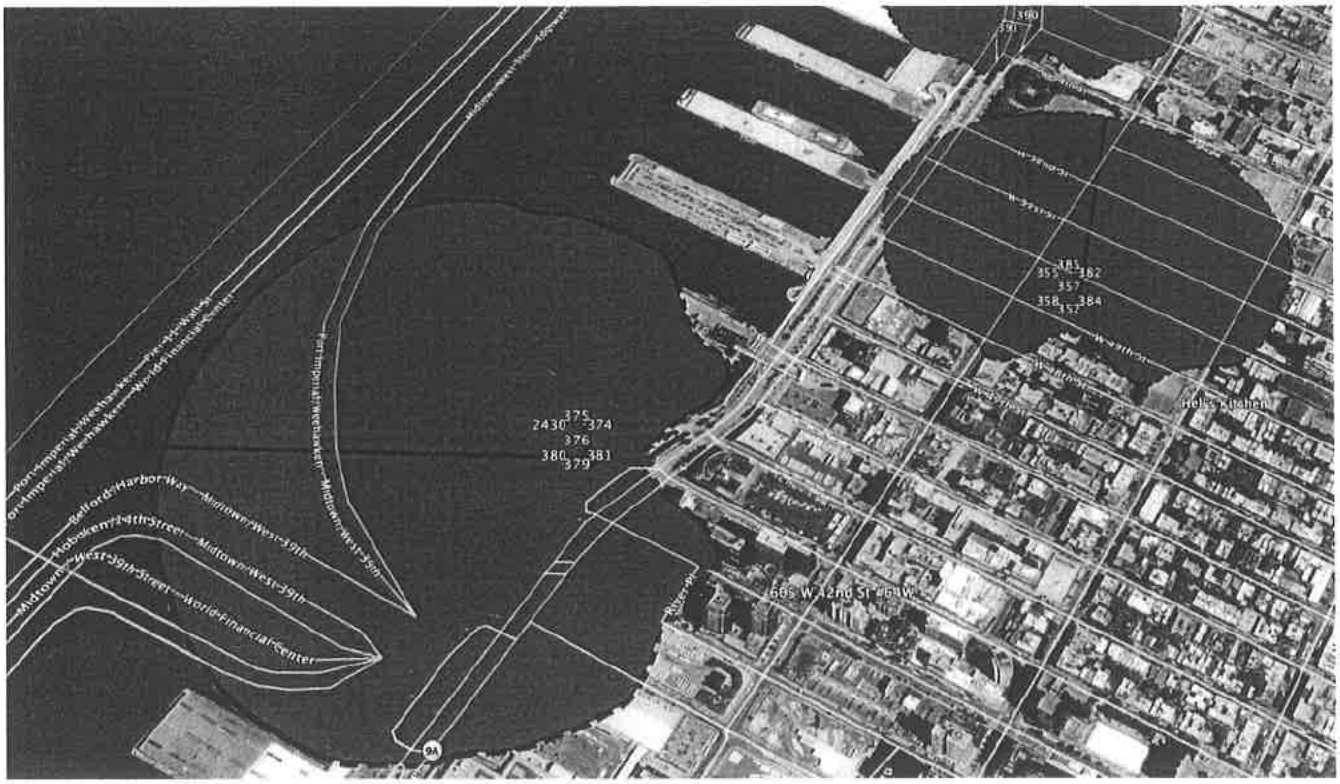
These records mean the owner of the AT&T phone number [redacted] linked to Suspect Truglia was assigned a SIM card that was physically inserted into the iPhone X (5311). Someone removed the SIM card form this iPhone X and placed it inside the iPhone 6 (6461). After approximately 18 minutes, someone removed the SIM card from the iPhone 6 (6461) and put it back into the iPhone X (5311). This SIM card has remained inside the iPhone X (5311) since it was put back in.

I examined the call detail records for the phone number [redacted] and I noticed that 10-23-18 at 22:09:35 (UTC) the IMEI switched from 359407081422499 (iPhone 10) to the iPhone 6 (6461). This IMEI remained active on the account until it switched back to the original IMEI number on 10-25-18 at 01:35:16, approximately 2 hours 25 minutes later. This time span is reasonable to explain the victim losing reception on his/her phone, realizing what happened, contacting AT&T and disconnecting the illegally connected phone from their account.

I examined the geolocation data provided by AT&T for two phone numbers discussed above.

The following pictures depict the AT&T cell phone towers the iPhone 6 (6461) was connected to during the approximate 2 hours and 10 minutes it was in control of the victim's account ([redacted]). The address [redacted] NY is placed for reference as it is listed as Suspect Truglia's residential address on his New York issued Identification Card.

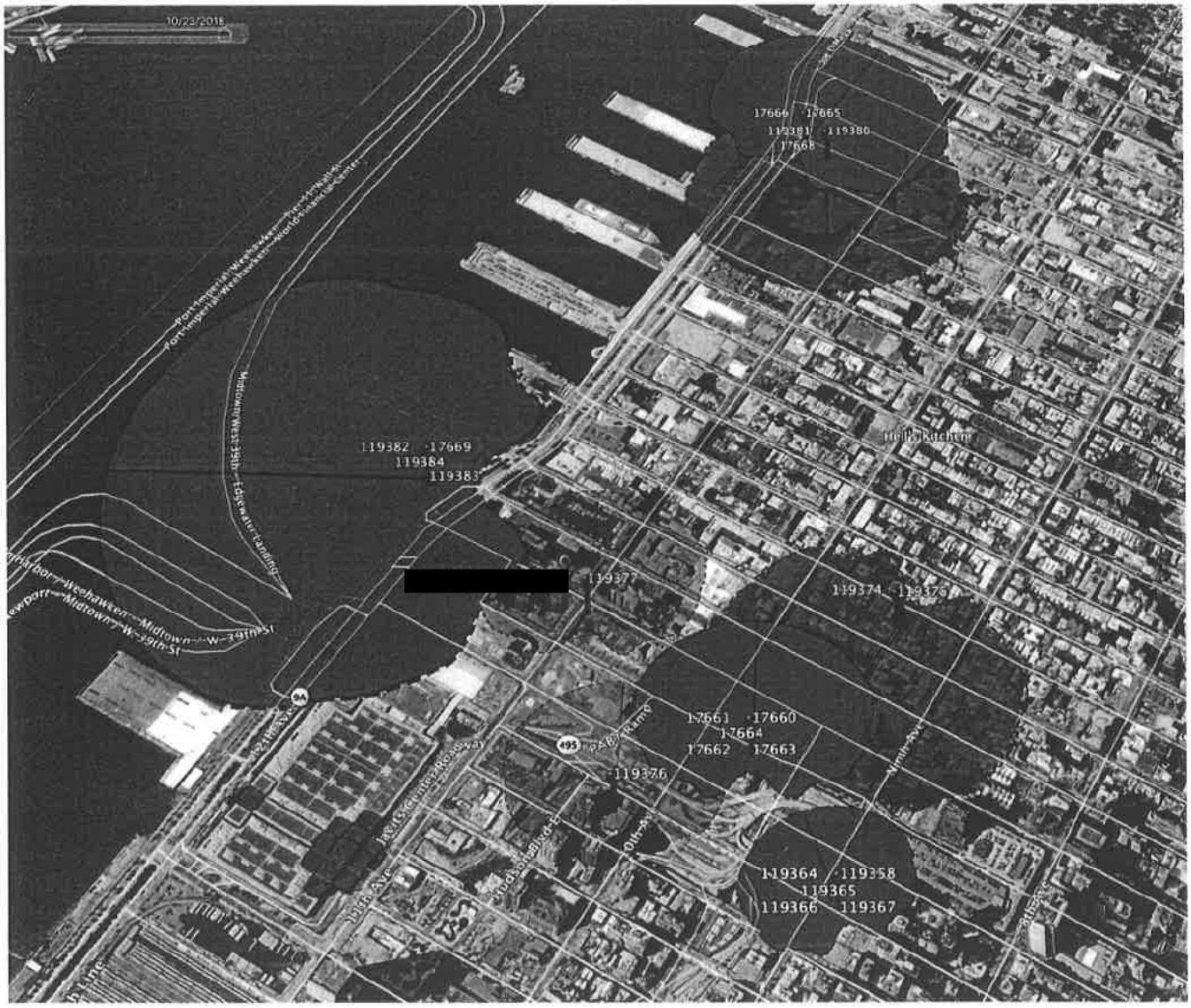
Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE



Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The tower to the west of [redacted] is identified by LTE ECGI-ENBID: 28486920-111277.

I further examined the geolocation data for Suspect Truglia's AT&T records for the same time period depicted above (approximately 2 hour 10 minute time window).



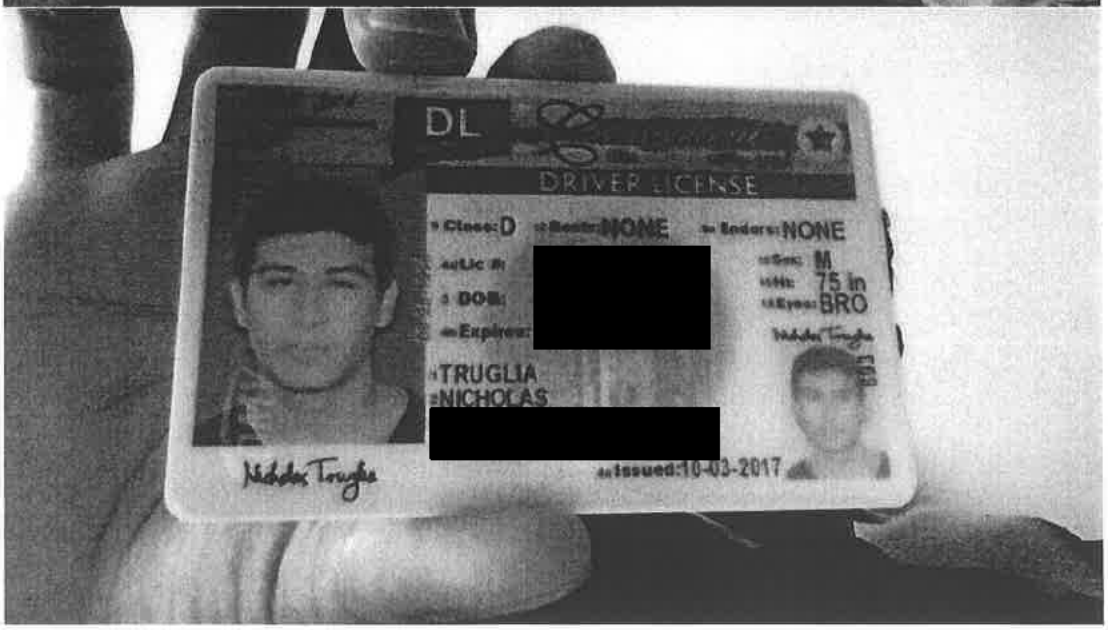
The same AT&T tower LTE ECGI-ENBID: 28486920-111277 was used by Suspect Truglia's AT&T account as well as several nearby towers. This is consistent with both devices being in the same geographical area at the same time.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

On 10-31-18 Coinbase provided additional information indicating that Truglia has previously been involved in account takeover activity. Coinbase informed REACT investigators that in mid-May 2018, Coinbase received an anonymous tip that someone was going to hack into the Coinbase account of Quinten Capobianco, who had previously died. After Coinbase secured the target account, an external attempt was made to access the account. Coinbase prompted the suspect to provide a photograph of himself holding his ID card as verification, and in response the suspect provided the photograph below.

The following three photos were provided as proof of identity on the other Coinbase accounts opened in Suspect Truglia's name:

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT: NARRATIVE



Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The following picture is from Suspect Truglia's New York Identification, which was obtained through a law enforcement database.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

DMV Photo Request

DMV Photo

Subject Information	
Name:	TRUGLIA,NICHOLAS,S
ClientID:	161405797
Case Number:	108711
DMV Transaction Number:	756281
DMV Transaction Date/Time:	2018-11-05 15:38:31:767

Back

I believe all of the pictures depicted above are of Suspect Truglia.

Based on this information, I believe Suspect Truglia attempted to access the deceased person's Coinbase account. This behavior is consistent with the SIM Swapping described in this report as the ultimate goal of the SIM Swapping is to steal cryptocurrency.

Based on the information above, I believe Suspect Truglia to have been in possession of the iPhone 6 (6461) and iPhone X (5311) described above and is responsible for conducting the SIM Swaps listed on page 1 of this report. See Detective Tuttle's Original report for further information.

END REPORT

PLEO:

Sgt. S. Tarazi- 2029

EXHIBIT C

About Our Privacy Policy

Whenever you do something like buy one of our products, watch a show or download an app, information is created. Because we know your privacy is important, we have a Privacy Policy to explain how we collect, use and protect that information. There's a quick summary below, and the actual policy is written in **an easy to understand "Frequently Asked Questions" (FAQ) format (/sites/privacy_policy/terms)**. We want to simplify this explanation, so you can make informed choices about your privacy, and then spend the rest of your time enjoying our products and services.

Revised February 15, 2019

A Quick Summary of Our Privacy Policy

Our Privacy Policy applies to your use of all products, services and websites offered by AT&T and our AT&T affiliates, such as DIRECTV, unless they have a different privacy policy. Because some apps, including some AT&T and DTV branded apps, require additional information, or use information in different ways, they may have their own privacy policies and/or terms and conditions. These apps may also offer you additional choices for managing your personal information.

Back to Top

Our privacy commitments

- We don't sell your Personal Information to anyone for any purpose. Period.
- We keep your Personal Information in our business records while you are a customer, or until it is no longer needed for business, tax or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.

Back to Top

Here's some of the information we collect:

- **Account Information** includes your name, address, telephone number, e-mail address, service-related details such as payment data, security codes, service history and other information like that;
- **Network Performance & Usage Information** tells us how you use our networks, our products and our services, and how well our equipment and networks are performing;
- **Web Browsing & Wireless Application Information** tells us about the websites you visit and the mobile applications you use on our networks;
- **Location Information** tells us where your wireless device is located, as well as your ZIP-code and street address;
- **TV Viewing Information** tells us about which programs you watch and record and similar information about how you use our video services and applications.

Back to Top

Here are the three basic ways we collect it:

- We get information from you when you do things like make a purchase from us;
- We collect it from how you use our products and services;
- We obtain information from other sources, like credit agencies, marketing companies, and other service providers.

Back to Top

Here are just some of the ways we use it. To:

- Provide services and improve your customer experience;
- Send you bills for your services;
- Respond to your questions;
- Address network integrity, help in fraud prevention and network and device security issues;
- Do research and analysis to maintain, protect, develop and improve our networks and services;
- Let you know about service updates, content, offers and promotions that may be of interest to you;
- Improve entertainment options;

- Deliver Relevant Advertising;
- Create External Marketing & Analytics Reports;
- Assist in the prevention and investigation of illegal activities and violations of our Terms of Service or Acceptable Use Policies.

Back to Top

Some examples of who we share your Personal Information with:

- **Across our companies** to give you the best customer experience and to help you get everything we have to offer.
- **Other, non-AT&T companies that perform services on our behalf** only as needed for them to perform those services. We require them to protect your information consistent with our Policy.
- **With other companies and entities, to:**
    - Respond to 911 requests and other emergencies or exigencies;
    - Comply with court orders and other legal process;
    - Assist with identity verification, and preventing fraud and identity theft;
    - Enforce our agreements and property rights;
    - and Obtain payment for products and services including the transfer or sale of delinquent accounts to third parties for collection

Back to Top

Understanding Personal, Anonymous & Aggregate Information

- What is Personal Information? Information that identifies or reasonably can be used to identify you.
- What is Anonymous Information? This is information that doesn’t identify you and can't reasonably be used to identify you specifically.
- What is Aggregate Information? We take a whole bunch of people’s data and combine it into anonymous groups or categories.
- How do we use this information? We use and share this information in many ways including research, analysis, retail marketing, and advertising. This data is also included in External Marketing & Analytics Reports.
- Want to learn more? Go **here (/sites/privacy_policy/terms#aggregate)**.

Back to Top

Our Online Privacy Policy for Children

- We want you to know that we don't knowingly collect personally identifying information from anyone under the age of 13 unless we first obtain permission from the child's parent or legal guardian.

Back to Top

Your Choices & Controls

- For information about children's safety and parental controls, view our **AT&T Smart Controls and DIRECTV Parental Controls (https://www.att.com/shop/wireless/smartcontrols.html)**.
- You have choices about certain types of advertising you get from us;
- You can control whether your Anonymous Information is used in our External Marketing & Analytics Reports;
- You can choose whether to receive marketing calls, e-mails or text messages or certain other communications from us;
- You have a choice about how we use your Customer Proprietary Network Information.

Back to Top.

Visit our **Privacy Policy (/sites/privacy_policy/full_privacy_policy)** for more information.

- **Definitions (/sites/privacy_policy/terms#definitions)**
- **Scope of this Policy (/sites/privacy_policy/terms#scope)**
- **The Information We Collect, How We Collect It, And How We Use It (/sites/privacy_policy/terms#collect)**
- **Information Sharing (/sites/privacy_policy/terms#sharing)**
- **Online Activity Tracking and Advertising (/sites/privacy_policy/terms#tracking)**
- **Location Information (/sites/privacy_policy/terms#location)**
- **Aggregate and Anonymous Information (/sites/privacy_policy/terms#aggregate)**
- **External Marketing & Analytics Reports (/sites/privacy_policy/terms#analytics)**
- **Online Privacy Policy for Children (/sites/privacy_policy/terms#children)**
- **Data Protection & Security (/sites/privacy_policy/terms#protection)**
- **Changes (/sites/privacy_policy/terms#changes)**
- **Choices & Controls (/sites/privacy_policy/terms#controls)**

- **How to Contact Us (/sites/privacy_policy/terms#contact)**

Your California Privacy Rights
California Civil Code Section 1798.83 entitles California customers to request information concerning whether a business has disclosed Personal Information to any third parties for their direct marketing purposes. As stated in this Privacy Policy, we will not sell your Personal Information to other companies and we will not share it with other companies for them to use for their own marketing purposes without your consent.

California Web Site Data Collection & "Do Not Track" Notices

Web Site Data Collection: We do not knowingly allow other parties to collect personally identifiable information about your online activities over time and across third-party web sites when you use our websites and services. We provide information about the opt-out choices available to customers, and the opt-out choices provided by certain third-party website and mobile application analytics companies we use **here (/sites/privacy_policy/rights_choices)**.

"Do Not Track" Notice: Because the providers of "do not track" and similar signals do not yet operate according to common, industry-accepted standards, we currently do not respond to those signals. For more information on Do Not Track, please visit **www.allaboutdnt.com (http://www.allaboutdnt.com/)**.

California customers who wish to request further information about our compliance with these requirements, or have questions or concerns about our privacy practices and policies may contact us at **privacypolicy@att.com (mailto:privacypolicy@att.com)**, or write to us at AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 1033, Dallas, TX 75202.

Back to top

AT&T Privacy Policy FAQ

Our AT&T Privacy Policy in easy to understand, FAQ format.

We understand that everyone thinks that privacy policies are long, complicated and

difficult to understand. So we're going to try to make this as simple as possible.

What is the purpose of AT&T's Privacy Policy? Whenever you do something like buy or use one of our products or services or visit our websites, information is created. Because we know privacy is important to you, we have the AT&T Privacy Policy to explain how we collect, use, protect, and share that created information. Thus, the main purpose of the Policy is to help you understand our relationship and how we are able to deliver and improve the services we offer.

How should this Policy be used? We encourage you to read the whole policy so you will understand fully our relationship. To find specific information, here is an outline of where you will find answers to your questions about key topics:

Visit these links for more information.

- **Definitions**
- **Scope of this Policy**
- **The Information We Collect, How We Collect It, And How We Use It**
- **Information Sharing**
- **Online Activity Tracking and Advertising**
- **Location Information**
- **Aggregate and Anonymous Information**
- **External Marketing & Analytics Reports**
- **Online Privacy Policy for Children**
- **Data Protection & Security**
- **Changes**
- **Choices & Controls**
- **How to Contact Us**

Definitions

Let's start with what we mean when we say:

Aggregate Information: We combine individual information into anonymous groups of customers or users. One way to think of it is in terms of a survey or opinion poll. Aggregate information would tell you that 80 percent of the people voted for a candidate, but not who actually voted. These groups are large enough to reasonably prevent individuals from being identified.

Anonymous Information: Information that doesn't directly identify and can't reasonably be used to identify an individual customer or user. We treat identifiers like cookies, advertising identifiers, device identifiers, and household identifiers as Anonymous Information except in circumstances where they can be used to identify you.

AT&T: Throughout this Policy, references to “AT&T,” “we,” “us,” and “our” include the family of AT&T companies around the world except affiliates or applications with a separate privacy policy.

Customer: Anyone who purchases or uses our products or services. When a customer purchases retail products or services for use by others, like a family account, those family members also are customers.

Mobile Application: A software application that runs on smartphones, tablet computers or other mobile devices and that allows users to access a variety of services and information.

Personal Information: Information that directly identifies or reasonably can be used to figure out the identity of a customer or user, such as your name, address, phone number and e-mail address. Personal Information does not include published listing information.

Relevant Advertising: Creates aggregate audience segments based on non-personally identifiable information about customers (like age, ethnicity, income range, a particular geographic area, and their interests) to serve advertising that is more likely to be useful to those audience segments. "Online behavioral advertising" is one type of Relevant Advertising. It uses interest categories based on the websites visited by people who are not personally identified to deliver advertising online.

Third-Party Services: Services from third-party service providers other than AT&T, such as banks or roadside assistance companies.

User: Anyone who visits our websites or uses our mobile applications.

Website: And other terms like "Internet site," "site" and "web page" all mean the same thing, namely any page or location on the Internet, no matter what device (cell phone, tablet, laptop, PC, etc.) or protocol (http, WAP, ftp or other) is used to access the page or location.

Back to Top.

Questions about the Scope of this Policy

1. **To whom does the Policy apply?**

This Privacy Policy applies to customers and users of AT&T products and services, except customers and users of products or services provided by an affiliate or an application with a different privacy policy.

2. **What does this Policy cover?**

This Privacy Policy covers our practices regarding the information we collect about our customers and users (how we collect it and how we use it). Use of our products and services, as well as visits to our websites, are subject to this Privacy Policy.

3. **Do you have any Privacy Policies other than this one?**

Yes. Some AT&T affiliates or applications may have separate privacy policies that describe how they collect, use and share information they collect from their customers and users. When we share Personal Information with those affiliates or combine it with information from those applications we protect it in a way consistent with this Privacy Policy.

Additionally, some of our applications may have terms and conditions that describe other privacy commitments or choices in addition to those in this Privacy Policy.

Some areas outside the United States require us to work a little differently. In that case, we may adopt separate privacy policies as necessary to reflect the requirements of applicable local laws.

The Joint AT&T EchoStar Privacy Policy for AT&T|DISH Network Customer Account Information remains in effect for AT&T|DISH subscribers.

4. **What about my family members and other users of my AT&T account? Does this Policy apply to them?**

Yes. You're responsible for making sure all family members or other users under your account understand and agree to this Policy. Get everyone together and talk about it. Or, send it by e-mail to make sure they're on board. Hang it on the fridge. Up to you, just share it!

5. **When is information not covered by this Policy?**

If you purchase or use the products or services of an AT&T affiliate that has a different privacy policy than this one, that privacy policy will apply.

Additionally, this Privacy Policy does not apply any time you give information to companies other than AT&T. Some examples are:

- When you use a non-AT&T Wi-Fi service;
- When you download applications or make purchases from other companies while using our Internet or wireless services;
- When you go to a non-AT&T website from one of our websites or applications (by clicking on a link or an advertisement, for example);
- When you give your information to another company through a website co-branded by AT&T but controlled by the other company;
- If you use public forums - such as social networking services, Internet bulletin boards, chat rooms, or blogs - the information is publicly available, and we cannot prevent distribution and use of that information by other parties;
- Information about your location, usage and the numbers you dial when you're out and about and roaming on the network of another company;
- When you purchase or use non-AT&T products (such as wireless devices, internet browsers and mobile applications) in combination with our services;
- When we license our brand to other companies for their use in marketing and selling certain non-AT&T products and services, information you give those companies is not covered by this Policy.

6. **Can my information be covered by this Policy and other privacy policies at the same time?**

Yes, that can happen. For example:

Sometimes we will work with other, unaffiliated companies to provide a service. In that case your information may be subject to this Policy and that of the other company. For example, you purchase one of our products or services from a retailer like Best Buy or Amazon.com, any information you provide to them may be subject to both their policy and ours.

If you connect to our Wi-Fi service through another network, such as one provided in a hotel, airport or other venue, any information collected from your use of that network could be subject to either the AT&T Privacy Policy or the venue policy, and sometimes both. The same thing applies if you connect to our network through your employer's corporate network, or any network operated by a non-AT&T company.

We think it's a great idea to take a look at the privacy policies of any companies you do business with to learn how they use your information.

7. **What about business customers?**

We may have written product or service agreements with our business customers that contain specific provisions about confidentiality, security or handling of information. When one of these agreements differs from or conflicts with this Policy, the terms of those agreements will apply. In all other instances, the terms of this Policy apply.

Back to Top.

Questions About The Information We Collect, How We Collect It, And How We Use It

1. **What information do you collect?**

We may collect different types of information based on your use of our products and services and on our business relationship with you.

- **Account Information:**
  - **Contact Information** that allows us to communicate with you. We get this information when you order or register for our services. This would include information like your name, address, telephone number and e-mail address.
  - **Billing Information** related to your financial relationship with us, such as the services we provide to you, the telephone numbers you call and text, your payment history, your credit history, your credit card numbers, Social Security number, security codes and your service history.
- **Technical & Usage Information** related to the services we provide to you, including information about how you use our networks, services, products or websites. Some examples include:

    - **Equipment Information** that identifies the equipment on our networks, such as equipment type, device identifiers, device status, serial numbers, settings, configuration and software.
    - **Network Performance & Usage Information** about the operation of the equipment, services and applications you use on our networks. Examples of this might include wireless device location, the number of text messages sent and received, voice minutes used, calling and texting records, bandwidth used, and resources you use when uploading, downloading or streaming data to and from the Internet. We also collect information like transmission rates and delays, data associated with remote monitoring services and security characteristics.
        - Some Network Performance & Usage Information and some Billing Information is **Customer Proprietary Network Information or "CPNI."** Unique rules apply to CPNI. **Go here (/sites/privacy_policy/rights_choices#cpni)** to learn more about what it is, how we use it and the choice you can make about that use.
    - **Web Browsing & Mobile Application Information** such as IP addresses, URLs, data transmission rates and delays. We also learn about the pages you visit, the time you spend, the links or advertisements you see and follow, the search terms you enter, how often you open an application, how long you spend using the app and other similar information.
- **Location Information** includes your ZIP-code and street address, as well as the whereabouts of your wireless device. Location information is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies, including the satellites that comprise the Global Positioning System.
- **TV Viewing Information** is generated by your use of any of our satellite or IPTV (U-verse) services. These services may include video on demand, pay per view, DVR services, applications to watch your TV on the go for tablet or smartphone (such as the TV Everywhere app) and similar AT&T services and products, including the programs and channels you and those in your household watch and record, the times you watch and how long you watch. It also includes information like the interactive channels and games provided by U-verse or DIRECTV. We also collect information related to your use and interaction with the equipment in your home, including the TV receivers, set top boxes, remotes and other devices you may use to access our services.

2. **How Do You Collect Information?**

In three basic ways:

- **You Give It To Us** when you make a purchase or set up an account with us;
- **We Automatically Collect Information** when you use our networks, products and services. For example, we use network tools to collect your call records; we collect wireless device location from our networks and from your device; and we also use **cookies (/sites/privacy_policy/cookies_and_other_technologies)**, web server logs and other technologies.
- **We Obtain Information from Outside Sources** like credit reports, marketing mailing lists, and commercially available geographic and demographic information along with other publicly available information, such as public posts to social networking sites.

3. **How Do You Use This Information?**

We use your information to improve your experience and to make our business stronger. Some examples include:

- Providing and managing your services, responding to your questions and addressing problems;
- Delivering customized content, or advertising, such as personalized offers for products and services that may be of interest to you;
- Communicating service updates, offers and promotions;
- Protecting network integrity and security, ensuring quality control, optimizing capacity and preventing misuse;
- Network enhancement planning, engineering and technical support;
- Conducting research and analysis for maintaining, protecting and developing our networks and our services;
- Preventing illegal activities, suspected fraud, and potential threats to our networks and our customers' networks;
- Investigating violations of our Terms of Service, Acceptable Use Policies, or other service conditions or restrictions; and
- Protecting the safety of any person.

4. **Do you use the information I store using one of your cloud services?**

We only use it to provide you with that service, unless we first get your permission to use it for something different.

Back to Top

Questions About Information Sharing

1. **Do you provide information for phone books and Caller ID?**

Yes and No.

Yes, we share the names, addresses and telephone numbers of our wireline telephone and U-verse Voice customers with businesses that publish directories and provide directory assistance services. We are required by law to do that. You may **contact us (http://about.att.com/sites/privacy_policy/terms#contact)** and we honor your request for non-published or non-listed phone numbers. Once we provide published listing information to those businesses, they may use, sort, package, repackage and make it available again in different formats to anyone.

Yes, we also provide wireline and wireless calling name and number information for CallerID, and related services like Call Trace, which allow a person receiving a call to obtain the name and number of the party calling them.

No, we do not give listing information for wireless numbers to phone book publishers or directory assistance services without your permission.

2. **Do you share my Personal Information internally?**

Yes. Our products and services are developed, managed, marketed and sold by a variety of our affiliated companies. We may share Personal Information internally, including with affiliated companies that may have different privacy policies. When we do this we require the affiliated company or companies to protect the Personal Information in a way consistent with this Privacy Policy. We may also combine Personal Information with data derived from an application that has a different privacy policy. When we do that, this Privacy Policy applies to the combined data set. Sharing information in these ways helps us offer you the high quality, seamless and innovative range of products you have come to expect from us. Some of these include:

- Wireless voice, data, Internet, home security, automation and remote monitoring services provided by AT&T Mobility and AT&T Digital Life; and
- The suite of satellite and IPTV services, Voice and High Speed Internet Access services offered by our companies.

If the affiliate relationship with one of our AT&T subsidiaries is not clear, information sharing with that subsidiary is handled as though it is a non-AT&T company. The relationship between AT&T branded companies can typically be identified through the use of the AT&T name or brand, the use of the AT&T "globe" logo, or through advertising, cross-promotional offers, or widely reported news or information in the press or social media that highlights the company as an AT&T affiliate (like Xandr and our highly publicized merger with the Time Warner family, now called **WarnerMedia (/ecms/dam/sites/Privacy%20Policy/WarnerMedia%20Affiliates.pdf)**). Affiliated companies that are not publicly recognized as part of the AT&T family of companies are treated as though they are non-AT&T companies for purposes of information sharing under this policy.

3. **Do you share my Personal Information with other non-AT&T companies for them to market to me?**

We will only share your Personal Information with other non-AT&T companies for them to use for the marketing of their own products and services when we have your consent.

4. **Are there any other times when you might provide my Personal Information to other non-AT&T companies or entities?**

Yes. We share your Personal Information with other, non-AT&T companies that perform services for us, like processing your bill. Because we take our responsibility to safeguard your Personal Information seriously, we do not allow those companies to use it for any purpose other than to perform those services, and we require them to protect it in a way consistent with this Privacy Policy. Companies that perform these services may be located outside the United States or the jurisdiction where you reside. If your Personal Information is shared with these companies, it could be accessible to government authorities according to the laws that govern those jurisdictions. There are also occasions when we provide Personal Information to other non-AT&T companies or other entities, such as government agencies, credit bureaus and collection agencies, without your consent. Some examples include sharing to:

- Comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements, and to enforce our legal rights or defend against legal claims;
- Obtain payment or make refunds for products and services that appear on your AT&T billing statements, including the transfer or sale of delinquent accounts or refund obligations to third parties for collection or payment.

- Enforce our agreements and protect our rights or property;
- Assist with identity verification and e-mail address validation;
- Respond to lawful requests by public authorities, including to meet national security or law enforcement requirements;
- Notify, respond or provide information (including location information) to a responsible governmental entity in emergency or exigent circumstances or in situations involving immediate danger of death or serious physical injury; and
- Notify the National Center for Missing and Exploited Children of information concerning child pornography of which we become aware through the provision of our services.

5. **Do you share my personally identifiable TV Viewing Information with other, non-AT&T companies?**

We don't share your personally identifiable TV Viewing Information with other non-AT&T companies for them to use for the marketing of their own products and services without your consent. We are required to notify you about the special requirements we must follow when it comes to sharing your personally identifiable TV Viewing Information in response to a Court Order:

Notice Regarding Disclosure of Personally Identifiable Information of Satellite and IPTV Subscribers in Response to A Court Order

- In the case of a court order obtained by a non-governmental entity, we are authorized to disclose personally identifiable information collected from TV subscribers as a result of the subscriber's use of TV service only after providing prior notice to the subscriber.
- In the case of a court order obtained by a governmental entity, we are authorized to disclose personally identifiable information collected from TV subscribers as a result of the subscriber's use of TV service only if, in the court proceeding relevant to the order:
    - The governmental entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
    - The subject of the information has an opportunity to appear and contest the governmental entity's claim; and
    - We have provided notice to the subscriber as required by applicable state law.

Back to Top

Questions About My Information and Advertising

1. **Do you use my information to send me advertising?**

Yes. We may use information like the preferences you have expressed and interests you have demonstrated on our websites, in our stores and through use of our products and services, to provide you with marketing information and advertisements for our products and services. Those ads may be delivered on our websites and mobile applications. This is called "first party" advertising. It is part of our service relationship and you are not able to opt-out from this type of advertising.

We or our advertising partners may use **Anonymous Information gathered through cookies and similar technologies (/sites/privacy_policy/cookies_and_other_technologies)**, as well as other Anonymous Information and Aggregate Information that either of us may have to help us tailor the ads you see on non-AT&T sites. For example, if you see an ad from us on a non-AT&T sports-related website, you may later receive an ad for sporting equipment delivered by us on a different website. This is called Online Behavioral Advertising, which is a type of Relevant Advertising.

2. **Do you use my information for other types of Relevant Advertising?**

Yes. We may also use information we get through your use of our products and services, from our advertising partners, and information like your age and gender to deliver Relevant Advertising that is not Online Behavioral Advertising. We combine your Anonymous Information with that of other users into aggregate "audience segments". These segments are based on particular interests and/or factual characteristics that everyone in that audience segment is likely to share. We might use that information to send you advertisements that are relevant to those interests or characteristics. When we use this information to deliver, and measure the effectiveness of, advertisements we associate it with other information, like advertising IDs, device IDs, or similar identifiers. We are careful to only use non-personally identifiable information to serve Relevant Advertising with aggregate audience segments that are large enough that you can't be identified individually.

In some cases you may agree to participate in advertising offers or programs through loyalty programs, when you download a mobile app, or other similar programs. In those cases, you will be told about the advertising program when you sign up. For more

information about those advertising programs, please consult the terms, conditions, and policies of the specific application or loyalty programs you are interested in or have joined.

3. **Do you use the location of my device for advertising purposes?**

Yes. We use information about the locations you visit in order to create combined wireless location interest characteristics that can be used to provide Relevant Advertising to you and others like you.

Location characteristics are types of locations - like "movie theaters". People who live in a particular geographic area (a city, ZIP-code or ZIP+ 4 code, for example) might appear to have a high interest in movies, thanks to collective information that shows wireless devices from that area are often located in the vicinity of movie theaters. We might create a "movies characteristic" for that area, and deliver movie ads to the people who live there.

We may associate your wireless device with a particular geographic area, such as a city, ZIP-code, or ZIP + 4 code, based on your billing address or the cell towers you connect with most frequently.

In addition to other privacy protections, the process we use to create our audience segment includes a requirement that the ZIP + 4 or other geographic area to which a wireless location is assigned must contain a minimum of 25 households. ZIP + 4 codes with less than 25 households are combined with other ZIP + 4 codes to satisfy this requirement.

4. **What's in it for me?**

Just like the name says, you get advertising that's more relevant to your interests. For example, if a particular audience segment, like adults between the ages of 21 and 25 with a certain income range, has demonstrated a greater interest in movies than other segments, we might send them a movie ad for a movie geared toward young adults. This is just one way we deliver content that's more relevant.

5. **How do you use information about the programs I watch on TV to advertise to me?**

We combine information about the shows that our customers are watching with their common interests to help us figure out what types of advertising they might be interested in seeing.

It sometimes works like this: We look at the group of people watching a particular show. We identify common characteristics within that group. We use those characteristics to identify and deliver advertising that might be most relevant to watchers of that TV show. We might also deliver that same advertising during shows that appear to have similar audiences.

6. **Do I ever have a chance to tell you what I'm personally interested in?**

Yes. With some programs offered or powered by AT&T you can sign up to receive text-message offers from businesses that are near your current location and match the interests you've selected. You can change your mind at any time and stop participating in these programs.

7. **What information do you provide to advertisers?**

We may provide reports to advertisers and other business customers about the success of its advertising campaigns. Those reports contain Anonymous Information about the number of times a particular ad was viewed, when it was viewed, whether it was viewed on a TV, a mobile device or a computer, demographics associated with the viewing audience and other similar information. Your Anonymous Information will not be included in aggregate reports about the success of Relevant Advertising campaigns if you have opted-out of Relevant Advertising delivered by AT&T.

Back to Top

Questions About Location Information

1. **What is location information?**

Exactly what it sounds like! It includes your ZIP-code and street address, as well as the whereabouts of your wireless device.

2. **How is it used?**

We use it in all kinds of ways, here are some examples:

- **We Provide Wireless Voice and Data Services:** We monitor, collect and use wireless location information, together with other information we get from our network and your wireless device, to maintain and improve our network. We also might use location information with your consent to provide you with a customized experience. For example, when you dial 411 Directory Assistance for a business telephone number, we might use your wireless location information to return the number of the business location closest to you.
- **Location Based Services (LBS):** Your device can be used to access a ton of services based on location. We offer these services via applications that have been pre-loaded or downloaded by you on your device. LBS also may be provided via text message or other functionality. We'll give you prior notice and ask for your consent when your location is used or shared. The form of consent may vary, but will be appropriate for the type of LBS you use.
- **LBS from other providers:** With your consent (to us or the other company) we also may enable LBS from other companies by providing location information to their developers or location service providers.
- We use it for **Advertising**

3. **How accurate is wireless location information?**

It depends on the technology we're using. For example, we can locate your device based on the cell tower that's serving you. The range could be up to 1,000 meters in any direction from the tower in urban areas, and up to 10,000 meters in rural areas. Wi-Fi networks provide more accurate location information, associating you with the place where the network is located - like a coffee shop - or to an area within or around that place.

Services such as 411, 911, a "friend locator" application or a navigation/mapping application, require more precise information. So for those we develop a more precise estimate of location by associating the serving cell tower ID with other information, like the latitude and longitude of the tower, radio frequency parameters, GPS information and timing differences in radio signals. Depending on a variety of factors, those methods may estimate the location of your device to within 30 to 1000 meters.

4. **Are you the only ones who can locate my wireless device?**

Other companies may also be able to locate your device. For example, your handset manufacturer and your operating system provider may be able to locate your device. If you download mobile applications, those apps may be able to obtain your location

directly from your handset or the operating system. Mobile applications that give you access to your employer's network may also give your employer the ability to locate your device.

We urge you to review policies of all providers.

Back to Top

Questions About Aggregate and Anonymous Information

1. **Where do you get Anonymous Information?**

Sometimes we'll collect information about how you use our products **using cookies and other similar technologies (/sites/privacy_policy/cookies_and_other_technologies)**. This information doesn't include your Personal Information and is considered anonymous.

When we collect information that identifies you personally, we may anonymize it for certain purposes. We remove data fields (such as name, address and telephone number) that can reasonably be used to identify you. We also use a variety of statistical techniques and operational controls to anonymize data. Anonymizing information is one of the tools we use to protect your privacy.

2. **Tell me more about aggregate information.**

Aggregate information is a form of Anonymous Information. We combine data that meet certain criteria into anonymous groups. For example, we might want to compare how customers in Beverly Hills, CA (or any city, county or ZIP-code) use their cell phones to how customers in Boulder, CO use their cell phones. In order to do that, we would combine customer data in each of the geographies into anonymous groups and look at all that aggregate data to understand how the two groups are different or similar.

3. **Do you share Anonymous or Aggregate Information?**

Yes, we may share this information with other companies and entities for specific uses, which may include:

- Universities, laboratories, think tanks and other entities that conduct networking, social, behavioral, environmental and other types of scientific research, for the purpose of creating fundamental new knowledge;

- Municipalities, government or other entities that may use this data for purposes such as municipal and transportation planning, and emergency and disaster response coordination;
- Advertisers and related companies for the delivery of advertising and to assess the effectiveness of advertising campaigns.

We share this information in external reports like our External Marketing & Analytics Reports and Metric Reports.

Back to Top

Questions About External Marketing & Analytics Reports

1. **Tell me more about the External Marketing & Analytics Program.**

We use aggregate information to create External Marketing & Analytics Reports that we may sell to other companies for their own marketing, advertising or other similar uses.

These reports may be a combination of information from wireless and Wi-Fi locations, TV Viewing, calling and texting records, website browsing and mobile application usage and other information we have about you and other customers. You have a choice about whether your Anonymous Information is included in the reports that we sell or provide to other companies.

Some examples of External Marketing & Analytics Reports include:

- Reports for retail businesses that show the number of wireless devices in or near their store locations by time of day and day of the week, together with demographic characteristics or other information about the users (such as device type, age or gender) in those groups.
- Reports that combine anonymous TV Viewing behaviors with other aggregate information we may have about our subscribers to create reports that would help a TV network better understand the audiences that are viewing their programs, those that are not, how frequently they watch, when they watch and other similar information; and
- Reports for device manufacturers that combine information such as device type, make and model with demographic and regional location information to reflect the popularity of particular device types with various customer segments.

2. **Do you provide companies with individual anonymous data as part of your External Marketing & Analytics Program?**

Yes. For example, we might share anonymous TV Viewing Information with media research companies that combine this data with other information to provide audience analysis services about what shows certain audience segments are watching. When we provide individual Anonymous Information to businesses, we require that they only use it to compile aggregate reports, and for no other purpose. We also require businesses to agree they will not attempt to identify any person using this information, and that they will handle it in a secure manner, consistent with this Policy.

3. **Do you use my Anonymous Information in other types of external reports?**

Yes, we may use your Anonymous Information to provide Metrics Reports to our business customers, advertisers, and service suppliers. These reports are considered part of the underlying service and we do not sell them to other customers or suppliers.

For example, if you connect to our Wi-Fi service in a hotel, airport or other venue you should know the operator of that venue is our business customer, and that we will provide that operator with Metrics Reports about usage of and communications with the Wi-Fi network in their location. Those reports contain statistical information like:

- The number of devices connecting to the Wi-Fi network, duration of Wi-Fi sessions and the amount of bandwidth used during those sessions; and
- Foot-traffic data, including the numbers of devices inside and outside the store at a given time; the number of new and frequent visitors; where visitors are located within the store (e.g., specific departments or other locations within the venue) and frequency of visits and time spent within the store.
- **NOTE:** When your wireless device is turned on, it regularly sends out signals that enable it to connect to cell towers, Wi-Fi access points or other technologies so that we (and others) are able to provide you with services. These signals can be used to determine your device location. You can turn Wi-Fi to the "off" position on the "settings" feature of your device to prevent the collection of these signals by Wi-Fi equipment in retail stores and other public places.

Another example, we also license video programming from content providers. As part of our agreement, we provide them with Metrics Reports. These reports contain combined measurements and statistical information related to the number of TV subscribers who watched or accessed a particular program at a particular time and other similar measurements.

Back to Top

Questions About Our Online Privacy Policy for Children

1. **Do you collect information about my children's use?**

We do not knowingly collect personally identifying information from anyone under the age of 13 unless we first obtain permission from the child's parent or legal guardian.

2. **What happens when my child is using an account not registered to them?**

Internet and wireless devices and services purchased for family use may be used by children without our knowledge. When that happens, information collected may appear to us to be associated with the adult customer who subscribes to our services and will be treated as the adult's information under this Policy.

3. **What can I do to help better protect my child's information?**

We encourage you to spend time online with your children, and to participate in and monitor their online activity. We have developed a website that offers safety and control tools, expert resources and tips designed to help you manage technology choices and address safety concerns. Please visit **AT&T Smart Controls (https://www.att.com/shop/wireless/smartcontrols.html)** for more information.

4. **What if my child has an AT&T e-mail sub-account?**

If you create an AT&T e-mail sub-account for a child under the age of 13:

- With your permission we collect your child’s name, nicknames and aliases, alternative e-mail address, birth date, gender and ZIP-code.
- We use the information collected on sub-accounts to create and maintain those accounts, for research, to customize the advertising and content seen on our pages and for other marketing purposes. Your child can use their AT&T e-mail address and password to log onto websites and online services provided by us, like **uverse.com (http://uverse.com/)**. We and our advertising partners may

collect and use information about customers who log onto those sites as described in the **"Questions about the Information We Collect, How we Collect It and How We Use It"** section of this Privacy Policy. A list of the advertising partners who collect information on our sites and the ability to opt-out of advertising provided by those partners is available **here (/sites/privacy_policy/rights_choices)**.

- We will not contact a child under the age of 13 about special offers or for marketing purposes without parental consent.
- You or your child can review, edit, update, and delete information relating to your child's sub-account and, if you no longer wish your child to have such an account, you can revoke your consent at any time, by logging on to manage your account **here (https://www.att.com/olam/loginAction.olamexecute?actionType=manage)**.

You may e-mail us at **privacypolicy@att.com (mailto:privacypolicy@att.com)**, call us at 800.495.1547 or write to us at AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 1033, Dallas, TX 75202 with any questions or concerns you may have about our Children's Online Privacy Policy.

Back to Top

Questions About Data Protection & Security

1. **Do we sell your Personal Information?**

No. We do not sell your **Personal Information (/sites/privacy_policy/terms#definitions)** to anyone, for any purpose. Period.

2. **How long do we keep your Personal Information?**

We keep your **Personal Information (/sites/privacy_policy/terms#definitions)** as long as we need it for business, tax or legal purposes. After that, we destroy it by making it unreadable or undecipherable.

3. **What safeguards does AT&T have in place?**

We've worked hard to protect your information. And we've established electronic and administrative safeguards designed to make the information we collect secure. Some examples of those safeguards include:

- All of our employees are subject to the **AT&T Code of Business Conduct (COBC) (https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf)** and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business - including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records. We take this seriously, and any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action. That includes dismissal.
- We've implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal Information. Some examples are:
    - Maintaining and protecting the security of computer storage and network equipment, and using our security procedures that require employee user names and passwords to access sensitive data;
    - Applying encryption or other appropriate security controls to protect Personal Information when stored or transmitted by us;
    - Limiting access to Personal Information to only those with jobs requiring such access; and
    - Requiring caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change the information.
    - Although we strive to keep your Personal Information secure, no security measures are perfect, and we cannot guarantee that your Personal Information will never be disclosed in a manner inconsistent with this Policy (for example, as the result of unauthorized acts by third parties that violate the law or this Policy).

4. Will you notify me in case of a security breach?

Laws and regulations guide us in how to give you notification when certain types of sensitive information are involved in a security breach. We will provide you with notice in accordance with these laws and regulations.

5. Can I review and correct my Personal Information?

Yes. We are happy to help you review and correct the Personal Information we have associated with your account and billing records within a reasonable time. Please see the **How to Contact Us About This Policy (http://about.att.com/sites/privacy_policy/terms#contact)** section.

Back to Top

Questions About Future Changes

1. **What happens if there is a change in corporate ownership?**

Information about our customers and users, including Personal Information, may be shared and transferred as part of any merger, acquisition, sale of company assets or transition of service to another provider. This also applies in the unlikely event of an insolvency, bankruptcy or receivership in which customer and user records would be transferred to another entity as a result of such a proceeding.

2. **Will I be notified if there are changes to this policy?**

We may update this Privacy Policy as necessary to reflect changes we make and to satisfy legal requirements. We will post a prominent notice of material changes on our websites. We will provide you with other appropriate notice of important changes at least 30 days before the effective date.

Back to Top

Your Choices & Controls

1. **You can choose not to receive some types of advertising online, on your satellite TV service or on your wireless device.**

   - **Relevant Advertising:** Opt-out of Relevant Advertising delivered by AT&T **here (https://cprodmasx.att.com/commonLogin/igate_wam/controller.do?TAM_OP=login&USERNAME=unauthenticated&ERROR_CODE=0x00000000&ERROR_TEXT=HPDBA0521I%20%20%20Successful%20completion&METHOD=GET&URL=%2Fpkmsvouchfor%3FATT%26https%3A%2F%2Fcprodx.att.com%2Fcmp%2Fcmpa%2Flogin.jsp&REFERER=https%3A%2F%2Fwww.att.com%2FCommon%2Fabout_us%2Fprivacy_policy%2Fprint_policy.html&HOSTNAME=cprodmasx.att.com&AUTHNLEVEL=&FAILREASON=&OLDSESSION)**.
   - **Online Behavioral Advertising:** Advertising that is customized based on predictions generated from your visits over time and across different

websites is sometimes called "online behavioral" or "interest-based" advertising. In accordance with industry self-regulatory principles, you can opt out of online behavioral advertising from companies who participate in the **Digital Advertising Alliance (http://www.aboutads.info/)** by going to their **Consumer Choice Page (http://www.aboutads.info/choices/#completed)** or by clicking on this icon **(http://www.aboutads.info/)** when you see it on an online ad. Opt-out of online behavioral advertising from many other ad networks at the **Network Advertising Initiative (NAI) site (http://www.networkadvertising.org/choices/)**.

- **Information about Cookies and Similar Technologies:** To limit collection of data on web sites that may be used for advertising, go **here (http://about.att.com/sites/privacy_policy/cookies_and_other_technologies)** for information on how to manage cookies and other similar technologies on your computer.
- **Advertising on att.net:** Opt-out of receiving interest-based advertising when using our att.net portal services powered by **Synacor (http://www.aboutads.info/choices)**. Opt-out of interest-based advertising on att.net from Yahoo! This covers att.net email and also the **Yahoo! (https://aim.yahoo.com/aim/us/en/optout/index.htm)** portal that is being retired.
- **Advertising Offers from Apps and Loyalty Programs:** In some cases you may agree to participate in advertising offers or programs through loyalty programs, when you download a mobile app, or other similar programs. For example, if you have the DIRECTV app, you can find out more about your choices concerning how your DIRECTV viewing information is used and shared **here (https://www.directv.com/DTVAPP/content/support/DTVAPP_policy)**.

2. **Do I have choices about receiving first party advertisements from AT&T?**

Because first party advertising is part of the service you receive when you visit our websites and use our mobile applications, we don't offer an opt-out for first party advertising.

3. **Can I choose not to receive marketing and other types of communication from AT&T?**

We realize that unwanted marketing contacts can be a hassle and we've worked hard to meet the expectations of customers and potential customers who have expressed a desire to limit certain types of solicitation communications from us.

E-Mail: Every marketing e-mail we send contains instructions and a link that will allow you to stop additional marketing e-mails for that product or service type. You also can unsubscribe from AT&T marketing e-mails **here (http://www.att.com/remove)**.

Text Messages: Opt-out of AT&T marketing text message contacts by replying "stop" to any message.

AT&T Consumer Telemarketing: Ask to be removed from our consumer telemarketing lists by contacting us at **one of the numbers listed here (/sites/privacy_policy/rights_choices#cpnicontact)**. You also can ask the AT&T representative to remove you from our telemarketing lists when you receive a marketing or promotional call from us.

AT&T Business Telemarketing: Where required by local laws and/or regulations, we honor requests to be removed from our telemarketing lists from business customers.

Federal Do Not Call: The FTC maintains a National Do Not Call Registry at **donotcall.gov (http://www.donotcall.gov/)**, and some states in the United States may maintain its own Do Not Call Registry. Putting your number on these Registries also may limit our AT&T telemarketing calls to that number.

Postal Mail: To review our Residential Do Not Mail Policy Statement and to limit postal mail solicitations, click **here (/sites/privacy_policy/att_consumer_marketing)**. You will still receive billing statements, legal notices, product updates and other similar correspondence, and you may still receive some promotional mailings.

All of our practices are designed to satisfy state, provincial and federal legal requirements limiting marketing contacts. Those laws and regulations - such as the requirements governing the state and federal

"Do Not Call" lists - generally permit companies to contact their own current and, in some cases, former customers, even when those customers are listed on the federal and state "Do Not Call" lists.

Automated Calls or Messages: In some cases, we will ask for your permission to send you automated calls or messages to your mobile phone. To opt out of these calls or messages from AT&T, please go to **Manage Your Privacy Choices (http://www.att.com/cmpchoice)**. As required or allowed by law, even if you opt out, AT&T may continue to contact you with automated calls or messages at the telephone number issued by us for certain important informational messages about your service. For example, we may need to let you know about a problem with your wireless service.

Restricting our use of your CPNI will not eliminate all types of our marketing contacts.

4. **Can I choose to exclude my Anonymous Information from your External Marketing & Analytics and other similar reports?**

Yes. Click **here (https://www.att.com/cmpchoice)** to opt-out. This opt-out also applies to the sharing of your Anonymous Information with other companies for their use in creating marketing and analytics reports. Although this opt out does not apply to Metrics Reports, it will apply if we combine Metrics Report information with other customer information (like demographics) to create reports that we provide to our business customers or service suppliers.

5. **What is DNS error assist?**

When you mistype a web address, or the address is not working, DNS Error Assist provides an automated list of similar pages – such as possibly the one you meant to type – for your consideration. The service is provided on your AT&T residential broadband connection, and you can opt-out **here (http://www.att.com/cmpchoice)**. If you opt-out, you will get a standard “no results found” error message instead of the error-assist page.

6. **Are there any other opt-out choices I should know about?**

We may use services provided by analytics companies to obtain information about website performance and how you use our mobile applications and other products and services. **Go here (http://www.aboutads.info/choices/)** for more information about the opt-outs made available by some of those vendors, and to make choices about participation. Based on your permission, we may share your mobile device location or other mobile subscriber information with third parties when you use Third-Party Services, such as to prevent fraud when making a bank transaction. If you want to change that permission, you can opt out directly with the third party or you can opt out by going to Manage Your Privacy Choices.

7. **These Choices and Controls also are available at http://about.att.com/sites/privacy_policy/rights_choices (/sites/privacy_policy/rights_choices).**

Back to Top

How to Contact Us About This Policy

We encourage you to contact us directly at either of these addresses below for any questions about this Privacy Policy.

- E-mail us at **privacypolicy@att.com (mailto:privacypolicy@att.com)**
- Write to us at AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 1033, Dallas, TX 75202.

For questions not related to privacy click on the "Contact Us" link at the bottom of any **att.com (http://www.att.com/)** page. You also can access your online account from the upper right hand corner of our home page at att.com for additional service options.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, you may contact our U.S.-based third-party ombudsperson program at **https://www.truste.com/consumer-resources/dispute-resolution/dispute-resolution-faqs/ (https://www.truste.com/consumer-resources/dispute-resolution/dispute-resolution-faqs/)**. If you are not satisfied with our resolution of any dispute, including with respect to privacy or data use concerns, please review our dispute resolution procedures at **http://www.att.com/disputeresolution (http://www.att.com/disputeresolution)**.

You also have the option of filing a complaint with the FTC Bureau of Consumer Protection, using an **online form (https://www.ftccomplaintassistant.gov)**, or by calling toll-free 877.FTC.HELP (877.382.4357; TTY: 866.653.4261). Other rights and remedies also may be available to you under federal or other applicable laws.

If you are a satellite TV subscriber, you also have certain rights under **Section 338(i) of the Federal Communications Act (http://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapIII-partI-sec338.pdf)**.

If you are a DIRECTV customer in Puerto Rico, you can exercise and manage your choices by visiting **https://www.directvpr.com/Midirectv/ingresar (https://www.directvpr.com/Midirectv/ingresar)** or by calling 787-776-5252.

Back to Top

Customer Proprietary Network Information (CPNI)

What is CPNI?

“CPNI” is information about your phone service from us. Your phone service could be a cell phone or any sort of home or business phone. The “information” is things like what kind of services you have, how you use them, or billing information. (Your telephone number, name and address are not considered CPNI.)

Back to Top

How is CPNI Used and Disclosed?

We do not sell, trade or share your CPNI with anyone outside of the AT&T family of companies* or our authorized agents, unless required by law (example: a court order).

We do use your CPNI internally, however. We may share information about our customers among the AT&T companies and our agents in order to offer you new or enhanced services. For example, we might offer a discount or promotion for Internet or TV services based on your CPNI.

Back to Top

How may I limit the use of my CPNI?

AT&T uses technology and security features, and strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI. It is your right and our duty under federal law to protect the confidentiality of your CPNI.

If you don't want AT&T to use your CPNI internally for things like offers, here is what you can do:

You can "opt out" online, at **att.com/ecpnioptout (http://att.com/ecpnioptout)**, or

You can call 800.315.8303, any time of day, and follow the prompts, or

You can speak to a service representative at 800.288.2020 (consumer) or 800.321.2000 (business).

For languages other than English and Spanish, please visit **world.att.com (http://world.att.com)**.

If you choose to restrict our use of your CPNI, it won't affect any of your services. You can change your mind at any time about allowing (or not allowing) us to use your CPNI, and we'll honor your decision until you change it again. If you do restrict your CPNI use, you may still get marketing from us, but it won't be from using CPNI.

** The AT&T Family of Companies are those companies that provide voice, video and broadband-related products and/or services domestically and internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services.*

Back to Top

Customer Service Contact Numbers

Wireless - 1-800-331-0500

Business - 1-800-321-2000

Residential - 1-800-288-2020

Spanish Language - 1-800-870-5855

Satellite TV Services - 1-800-DIRECTV or 1-800-531-5000

For assistance in other languages, please visit **world.att.com (http://world.att.com)**.

Legacy AT&T Consumer - 1-800-222-0300

Customers of the following AT&T family of companies may contact us directly using the following:

AT&T Internet Services - Customers can manage newsletter subscriptions or other e-mail communications from Yahoo! by modifying their AT&T Yahoo! Marketing Preferences.

Back to Top